Welcome to The 2022 Security Benchmark Report, which includes comparisons of all security organizations, sector reports, annual trends and achievements.
By Maggie Shein, Editor in Chief

Benchmarking allows security leaders to evaluate, check or compare how their position or function matches others in the industry. How many security employees do similar-sized companies in similar market sectors have within their organization? Did your peers see an increase in their security budget year-over-year? If so, by how much? Are security executives within your market sector responsible for many of the same programs you are responsible for?

Security leaders across all market sectors fill out The Security Benchmark Report — an in-depth survey which collects data on overall enterprise revenue or operating budget, security budgets, number of guarding personnel, security technologies, roles, responsibilities, reporting structures and much more — to gain real-world insight into what other security programs are doing.

The Security Benchmark Report is an editorial initiative that collects and reports on self-reported responses only. Our editorial goal is to provide security leaders with a free benchmarking program that can help them continue to evolve and grow their security program year after year.

The survey is filled out by security practitioners that have responsibility, at least in part, for physical security within their organization.

While The Security Benchmark Report aims to offer security programs insight into what their peers are doing, we understand that the metrics important to one team may be completely different than what's important to another team.

Therefore, the biggest benefit to filling out The Security Benchmark Report survey is that each security executive respondent receives the raw, anonymized data from the survey to compare and contrast across the industry or specific respondents within their sector based on any metric they wish.

For further data and comparisons beyond what is reported on these pages, fill out The Security Benchmark Report survey next year. The survey opens in February and closes in early July. Security magazine does not sell or share respondent information collected from this survey.
TABLE OF CONTENTS

4 MAIN REPORT / SECURITY ROLES & RESPONSIBILITIES
10 MAIN REPORT / SECURITY BUDGETS, SPENDING & MORE
12 MAIN REPORT / SECURITY GUARDING & OPERATIONS
14 MAIN REPORT / SECURITY-RELATED TRAINING & TECHNOLOGY
17 MAIN REPORT / SECURITY TEAMS USING METRICS
47 SECTOR / INFORMATION TECHNOLOGY & MEDIA
51 SECTOR / MANUFACTURING
55 SECTOR / PHARMA & BIOTECH
59 SECTOR / RETAIL & RESTAURANT
63 SECTOR / UTILITIES & DISTRIBUTION
67 THE 2022 ACHIEVERS / TRAINING
68 THE 2022 ACHIEVERS / DEI
69 THE 2022 ACHIEVERS / BUSINESS ENABLERS
70 THE 2022 ACHIEVERS / NEW INITIATIVES
71 THE 2022 ACHIEVERS / RETENTION & DEVELOPMENT
72 THE 2022 ACHIEVERS / TECHNOLOGY
73 THE 2022 SECURITY BENCHMARK REPORT / METHODOLOGY
SECURITY ROLES & RESPONSIBILITIES

Top 10 Biggest Issues / Concerns for Security Leaders

<table>
<thead>
<tr>
<th>RANK</th>
<th>Issues / Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workplace violence</td>
</tr>
<tr>
<td>2.</td>
<td>Business continuity and business resilience</td>
</tr>
<tr>
<td>3.</td>
<td>Staffing and training</td>
</tr>
<tr>
<td>4.</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>5.</td>
<td>Civil unrest, disturbances, riots, activists, targeted protests, etc.</td>
</tr>
<tr>
<td>6.</td>
<td>Risk and threat intelligence</td>
</tr>
<tr>
<td>7. (tie)</td>
<td>Crisis management</td>
</tr>
<tr>
<td>7. (tie)</td>
<td>COVID-19 (pandemics, etc.)</td>
</tr>
<tr>
<td>9.</td>
<td>Insider threat</td>
</tr>
<tr>
<td>10.</td>
<td>Supply chain security</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked about their top issues / concerns in 2022 and 2023 in regards to risk mitigation and enterprise security. The top 10 answers appear above in order. Honorable mentions include Theft, Security budget, and Natural disasters. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives Within the Enterprise

Respondents report where their security function reports to or resides within their organization.

- COO / Operations — 20%
- CRO / Risk / Legal / General Counsel — 19%
- CEO / President / Owner / Exec. Director — 13%
- CAO / Administration / Shared Services — 10%
- CFO / Finance — 9%
- Human Resources — 9%
- Other — 5%
- Facilities — 5%
- Board or Board Committee — 3%
- CIO / Information Technology — 3%
- CTO / Chief Technology Officer — 2%
- General Manager / Business Unit — 2%

The Security Benchmark Report respondents were asked where their security function reports to or resides within. The majority of security teams responding to this year’s Security Benchmark Report report to or reside within COO / Operations, followed closely by CRO / Risk / Legal / General Counsel. SOURCE: The Security Benchmark Report, November 2022
SECURITY ROLES & RESPONSIBILITIES

Title of Senior-Most Security Executive

<table>
<thead>
<tr>
<th>Title / Percent of Respondents</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director</td>
<td>29%</td>
</tr>
<tr>
<td>C-Level Executive</td>
<td>28%</td>
</tr>
<tr>
<td>Vice President / General Manager</td>
<td>24%</td>
</tr>
<tr>
<td>Senior Director</td>
<td>10%</td>
</tr>
<tr>
<td>Senior Manager</td>
<td>6%</td>
</tr>
<tr>
<td>N/A</td>
<td>3%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked to choose the title of their senior-most security executive within their enterprise. The choices, which are not exhaustive, are meant to generally group titles for comparison and include: C-Level Executive, Director, Senior Director, Senior Manager, Vice President / General Manager or Not Applicable (N/A). Among those choosing N/A were Police Chiefs, Managers and Supervisors. SOURCE: The Security Benchmark Report, November 2022

Geographic Security Responsibility

Respondents report which geographic areas they provide risk and security services to.

<table>
<thead>
<tr>
<th>Geographic Area</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>96%</td>
</tr>
<tr>
<td>Asia</td>
<td>49%</td>
</tr>
<tr>
<td>Europe</td>
<td>48%</td>
</tr>
<tr>
<td>South America</td>
<td>39%</td>
</tr>
<tr>
<td>Oceania (including Australia)</td>
<td>35%</td>
</tr>
<tr>
<td>Africa</td>
<td>32%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services to within their enterprise. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
SECURITY ROLES & RESPONSIBILITIES

Structure of Security
Respondents report on the structure of their security function within the overall organization.

- Centralized — 81%
- Decentralized — 9%
- Regional — 7%
- Other — 3%

The Security Benchmark Report respondents were asked if their security organization is Centralized, Decentralized or Regional. The majority of respondents reported their security organization as being Centralized. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another. Those respondents choosing Other reported working in single sites or a Partially Centralized and Partially Decentralized structure. SOURCE: The Security Benchmark Report, November 2022

Security’s Responsibilities
Here are the top 15 roles that security teams report owning or managing.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aligning security with the business</td>
</tr>
<tr>
<td>2</td>
<td>Asset protection / facilities protection</td>
</tr>
<tr>
<td>3</td>
<td>Civil unrest / disturbances / riots</td>
</tr>
<tr>
<td>4</td>
<td>Investigations</td>
</tr>
<tr>
<td>5</td>
<td>Liaison with public sector / law enforcement agencies</td>
</tr>
<tr>
<td>6</td>
<td>Loss prevention / goods protection</td>
</tr>
<tr>
<td>7</td>
<td>Security audits / surveys / assessments</td>
</tr>
<tr>
<td>8</td>
<td>Security contract management</td>
</tr>
<tr>
<td>9</td>
<td>Security operations center management</td>
</tr>
<tr>
<td>10</td>
<td>Security staff development &amp; training</td>
</tr>
<tr>
<td>11</td>
<td>Security strategy</td>
</tr>
<tr>
<td>12</td>
<td>Security technology &amp; integration</td>
</tr>
<tr>
<td>13</td>
<td>Targeted protests / activists / hate crimes</td>
</tr>
<tr>
<td>14</td>
<td>Terrorism / extremism</td>
</tr>
<tr>
<td>15</td>
<td>Workplace violence / active shooter prevention</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were given a list of 37 roles and responsibilities that may fall under the security function at an organization and were asked for the level of responsibility the team has over that role within their enterprise. These are the 15 most common job responsibilities (in alphabetical order) that the security function Owns / Leads or Manages, according to respondents. For this survey, Owning / Leading the responsibility means security both manages and funds the program, while Managing means security manages the program, but another group funds it. SOURCE: The Security Benchmark Report, November 2022
SECURITY ROLES & RESPONSIBILITIES

Organizational Responsibilities: Security Roles & Functions
Respondents report on responsibilities they hold, as well as the level of each responsibility.

<table>
<thead>
<tr>
<th>Function</th>
<th>Own / Lead</th>
<th>Manage</th>
<th>Support</th>
<th>Not Involved / Do Not Have or Do Not Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset protection / facilities protection</td>
<td>79%</td>
<td>13%</td>
<td>6%</td>
<td>2%</td>
</tr>
<tr>
<td>Brand protection / intellectual property / product protection / counterfeit / fraud protection</td>
<td>23%</td>
<td>11%</td>
<td>51%</td>
<td>15%</td>
</tr>
<tr>
<td>Business resilience (business continuity, emergency management, disaster recovery)</td>
<td>41%</td>
<td>15%</td>
<td>41%</td>
<td>3%</td>
</tr>
<tr>
<td>Business expansion support</td>
<td>13%</td>
<td>10%</td>
<td>62%</td>
<td>15%</td>
</tr>
<tr>
<td>Civil unrest / disturbances / riots</td>
<td>76%</td>
<td>9%</td>
<td>9%</td>
<td>6%</td>
</tr>
<tr>
<td>COVID-19 response</td>
<td>27%</td>
<td>14%</td>
<td>54%</td>
<td>5%</td>
</tr>
<tr>
<td>Cybersecurity / information technology security / data protection</td>
<td>10%</td>
<td>6%</td>
<td>62%</td>
<td>22%</td>
</tr>
<tr>
<td>Drug &amp; alcohol testing, background checks, other pre-employment screening (where applicable)</td>
<td>19%</td>
<td>9%</td>
<td>44%</td>
<td>28%</td>
</tr>
<tr>
<td>Duty of care / traveler protection &amp; support / executive protection</td>
<td>61%</td>
<td>7%</td>
<td>13%</td>
<td>19%</td>
</tr>
<tr>
<td>Emergency response &amp; planning</td>
<td>56%</td>
<td>16%</td>
<td>27%</td>
<td>1%</td>
</tr>
<tr>
<td>Event security</td>
<td>73%</td>
<td>13%</td>
<td>9%</td>
<td>5%</td>
</tr>
<tr>
<td>Investigations</td>
<td>62%</td>
<td>14%</td>
<td>21%</td>
<td>3%</td>
</tr>
<tr>
<td>Parking &amp; transportation security</td>
<td>50%</td>
<td>12%</td>
<td>25%</td>
<td>13%</td>
</tr>
<tr>
<td>Regulatory compliance / controls assurance &amp; verification / validation</td>
<td>15%</td>
<td>15%</td>
<td>57%</td>
<td>13%</td>
</tr>
<tr>
<td>Risk / threat assessments / risk management planning / enterprise risk management</td>
<td>56%</td>
<td>14%</td>
<td>29%</td>
<td>1%</td>
</tr>
<tr>
<td>Security audits / surveys / assessments</td>
<td>76%</td>
<td>13%</td>
<td>8%</td>
<td>3%</td>
</tr>
<tr>
<td>Security contract management (guards, technology integrators, contract employees)</td>
<td>71%</td>
<td>12%</td>
<td>11%</td>
<td>6%</td>
</tr>
<tr>
<td>Security staff development &amp; training</td>
<td>83%</td>
<td>8%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Security technology &amp; integration</td>
<td>70%</td>
<td>13%</td>
<td>13%</td>
<td>4%</td>
</tr>
<tr>
<td>Workplace violence / threat management / active shooter prevention</td>
<td>84%</td>
<td>8%</td>
<td>6%</td>
<td>2%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked to report on the security team’s roles and responsibilities within their organization. This year, we asked security leaders for the level of responsibility for each function within their organization with the following choices: Own / Lead Function: Security manages and funds the program; Manage: Security manages the program but another group funds it; Support: Security sets policy, consults on the program (or represents physical security perspective) but does not manage or fund the program; Not Involved: Company has the program but security is not involved in it; Do Not Have; Do Not Know. We have combined Not Involved / Do Not Have or Do Not Know responses for the purposes of this chart, however, 17 more responsibilities and breakdown of responses, in addition to those reported here, are included in the survey and are a part of the full report that respondents receive. One interesting note is that comparing COVID-19 responsibilities with 2021’s responses reveals a smaller number of respondents this year reporting Owning / Leading and Managing COVID-19 response, while a slightly higher percent report Supporting the efforts. One possible explanation could be that, now a few years into the pandemic, organizations have hired or diversified response efforts to in order to sustain pandemic efforts in the long term. SOURCE: The Security Benchmark Report, November 2022.
SECURITY ROLES & RESPONSIBILITIES

Do Security Teams Have a Charter or Policy / Policies Within the Enterprise that Clearly Define(s) the Role / Authority of Security?

- YES: 82%
- NO: 10%
- Under development: 8%


- YES: 69%
- NO: 15%
- Under development: 8%

Do Security Organizations Track / Maintain Security-Related Metrics / Analysis or Data to Help Determine Incident Response, Proper Staffing, etc.?

- YES: 82%
- NO: 6%
- Under development: 12%

SOURCE: The Security Benchmark Report, November 2022
SECURITY ROLES & RESPONSIBILITIES

Pre-Employment Screening Conducted Across the Enterprise

Respondents report on which pre-employment security checks the organization conducts.

- Criminal background — 93%
- Employment reference — 82%
- Personal reference — 68%
- Drug testing — 64%
- Military background — 57%
- Credit checks — 49%
- Social media reviews — 35%
- Other — 10%
- Don’t know — 3%

The Security Benchmark Report respondents were asked what security checks/testing the organization conducts as part of pre-employment screening. Respondents were allowed to indicate as many answers as applicable to their organization. Respondents were also able to choose Other (10%) or Don’t know (3%). The Don’t know answer is meant to give other security organizations knowledge into the roles/responsibilities/maturity of other security programs. For this question, other forms of screening indicated by respondents included education verification, media checks and DMV checks. SOURCE: The Security Benchmark Report, November 2022

Security Executive Insights

Is your highest security-related role within the organization responsible for both PHYSICAL SECURITY and CYBERSECURITY?

- Yes — 22%
- No — 78%

Is your highest security-related role within the organization ultimately responsible for both PHYSICAL SECURITY and HEALTH & SAFETY?

- Yes — 56%
- No — 44%

The Security Benchmark Report respondents are responsible, at least in part, for physical security within their organization. We asked survey respondents for more insight into the ever-evolving and changing roles of security, including whether their role within the organization is ultimately responsible for both physical security and health & safety, as well as physical security and cybersecurity. In 2021, only 14% of the Security Benchmark Report respondents reported being responsible for both physical security and cybersecurity, translating to a 57% increase in this year’s report. In 2021, 51% of respondents reported being responsible for both physical security and health & safety, translating to a 10% increase in this year’s report. SOURCE: The Security Benchmark Report, November 2022
**SECURITY BUDGETS, SPENDING & MORE**

### Average Security Budget as Percent of Revenue

<table>
<thead>
<tr>
<th>Sector</th>
<th>Security Budget as % of Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>2.9%</td>
</tr>
</tbody>
</table>

The average **security budget as a percent of revenue** among The Security Benchmark Report respondents was 2.9%.

The Security Benchmark Report captures information on security budgets and total reported revenue/operating budget in the overall organization. To calculate the security budget as a percentage of revenue across the enterprise, the security budget is divided by the total revenue. Companies that reported information on both security budget and total revenue are included in this number; however, if any numbers appeared inaccurately reported or incorrect, they were removed from the calculation. **SOURCE: The Security Benchmark Report, November 2022**

### Average Security Budget as a Percent of Revenue by Sector

See which sectors have the highest security budget as a percent of revenue on average.

- **Agriculture, Food & Beverage, Construction** — 4.9%
- **Business Services & Consulting** — 4%
- **Entertainment & Cultural Institutions** — 3.4%
- **Healthcare** — 3.1%
- **Aerospace & Defense** — 2.1%
- **Higher Education** — 1.9%
- **Retail & Restaurant** — 1.8%
- **Manufacturing** — 0.5%
- **Pharma & Biotech** — 0.5%
- **Information Technology & Media** — 0.4%
- **Banking & Insurance** — 0.3%
- **Utilities & Distribution** — 0.1%

Above is the average security budget as a percent of revenue by market sector. The Security Benchmark Report captures information on security budgets and total reported revenue / operating budget in the overall organization. To calculate the security budget as a percent of revenue across the enterprise, the security budget is divided by the total revenue. Companies that reported information on both security budget and total revenue are included in this number; however, if any numbers appeared inaccurately reported or incorrect, they were removed from the calculation. **SOURCE: The Security Benchmark Report, November 2022**
A majority of The Security Benchmark Report respondents reported an increased security budget compared with the previous year’s budget. In 2021, 66% of respondents reported an increased budget that year, while this year 69% of respondents reported an increased security budget year-over-year. SOURCE: The Security Benchmark Report, November 2022

If The Security Benchmark Report respondents indicated an increased security budget in 2022 compared with 2021, they were asked what percentage that budget increased. The average increase reported by those respondents for 2022 was 19%. If respondents indicated their security budget in 2022 decreased compared with 2021 they were asked for the percentage decrease. The average decrease reported by those respondents for 2022 was 11%. In 2021, the average increase in security budget was 14% and the average decrease in security budget was 21%. SOURCE: The Security Benchmark Report, November 2022

A majority of The Security Benchmark Report respondents reported an increased security budget compared with the previous year’s budget. In 2021, 66% of respondents reported an increased budget that year, while this year 69% of respondents reported an increased security budget year-over-year. SOURCE: The Security Benchmark Report, November 2022

How Much Did Security Budgets Change Year-Over-Year?
Respondents were asked how much their security budget increased or decreased compared with the previous year.

If The Security Benchmark Report respondents indicated an increased security budget in 2022 compared with 2021, they were asked what percentage that budget increased. The average increase reported by those respondents for 2022 was 19%. If respondents indicated their security budget in 2022 decreased compared with 2021 they were asked for the percentage decrease. The average decrease reported by those respondents for 2022 was 11%. In 2021, the average increase in security budget was 14% and the average decrease in security budget was 21%. SOURCE: The Security Benchmark Report, November 2022
Security Guarding & Operations

Use of Security Guards / Officers
What percentage of respondents using security officers have proprietary guards, contract guards or both?
Both proprietary and contract guarding — 34%
Contract guarding only — 33%
Proprietary guarding only — 33%

Of those The Security Benchmark Report respondents that reported using guard / officer forces at their organization, 34% of security leaders report using both proprietary and contract officer / guard forces, while 33% report having only proprietary guards and 33% reported having only third-party / contract guards. SOURCE: The Security Benchmark Report, November 2022

Do You Have a Security Operations Center (SOC)?
Yes — 68%
No — 32%

Security Operations Center Reach
Entire enterprise — 88%
Limited to a particular site or region — 12%

Overall, 88% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOCC) within their enterprise. Respondents that answered “Yes” to having a SOC were asked if their SOCs provide security and risk services to the entire enterprise or just a particular region or site. Overall, among all sectors, 88% of respondents that reported having a SOC offer those services to the entire enterprise. SOURCE: The Security Benchmark Report, November 2022
SECURITY GUARDING & OPERATIONS

What Services Do Security Operations Centers Provide?
Respondents report which services their security operations centers provide to their organization.

- Monitoring video surveillance and alarms — 94%
- Monitoring and triaging internal incidents reported — 87%
- Monitoring external events that may impact the enterprise — 87%
- Administering access control permissions and monitoring alarms — 85%
- Monitoring weather and alerting enterprise of potential impacts — 80%
- Answering and routing general inquiry phone calls — 76%
- Tracking executive travel and events — 57%
- Monitoring social media posts that name the enterprise and / or top executives — 54%
- Preparing risk assessments and situation reports — 53%
- Tracking business travel — 52%
- Developing and distributing travel security guidance — 52%
- Performing COVID-19 data collection and / or contact tracing — 39%
- Monitoring executives’ home security systems and responding to alarms — 34%
- Monitoring cyber-related incidents or threats — 23%

Among the 68% of The Security Benchmark Report respondents that reported having a global security operations center (GSOC) or security operations center (SOC), Security magazine asked respondents which services their SOCs provide to the enterprise, represented in the bar graph above. Respondents were able to choose as many responses as applicable. SOURCE: The Security Benchmark Report, November 2022
SECURITY-RELATED TRAINING & TECHNOLOGY

Money Spent on Security-Related Training by Sector

Here's the average money spent on security-related training broken out by sector.

- Healthcare — $208,800
- Retail & Restaurant — $190,000
- Manufacturing — $162,500
- Aerospace & Defense — $133,000
- Banking & Insurance — $76,000
- Information Technology & Media — $72,600
- Agriculture, Food & Beverage, Construction — $68,750
- Utilities & Distribution — $60,000
- Pharma & Biotech — $59,300
- Business Services & Consulting — $54,500
- Entertainment & Cultural Institutions — $25,500
- Higher Education — $16,500

Above is the average money spent on security-related training by sector, based on self-reported information from The Security Benchmark Report respondents. Outliers or information that appeared to be inaccurately reported were excluded from these calculations. SOURCE: The Security Benchmark Report, November 2022
SECURITY-RELATED TRAINING & TECHNOLOGY

Which of the Following Security-Related Training Did You Implement at Your Organization Last Year?

<table>
<thead>
<tr>
<th>Type of Training</th>
<th>Security Staff</th>
<th>Enterprise-Wide</th>
<th>Targeted Cross-Functional Group</th>
<th>Not Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis management</td>
<td>52%</td>
<td>27%</td>
<td>50%</td>
<td>15%</td>
</tr>
<tr>
<td>Emergency response</td>
<td>59%</td>
<td>36%</td>
<td>43%</td>
<td>10%</td>
</tr>
<tr>
<td>Executive protection</td>
<td>50%</td>
<td>6%</td>
<td>17%</td>
<td>39%</td>
</tr>
<tr>
<td>Insider threat</td>
<td>44%</td>
<td>23%</td>
<td>31%</td>
<td>30%</td>
</tr>
<tr>
<td>Investigation-related</td>
<td>60%</td>
<td>9%</td>
<td>28%</td>
<td>23%</td>
</tr>
<tr>
<td>Leadership development</td>
<td>62%</td>
<td>22%</td>
<td>26%</td>
<td>16%</td>
</tr>
<tr>
<td>Security technology</td>
<td>66%</td>
<td>18%</td>
<td>32%</td>
<td>17%</td>
</tr>
<tr>
<td>Workplace violence</td>
<td>57%</td>
<td>62%</td>
<td>43%</td>
<td>9%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked to report the security-related training they held within their enterprise in 2021. Respondents were able to choose multiple populations for each training if applicable. For example, in relation to Workplace violence, some organizations implemented training for both security staff as well as targeted cross-functional groups. Respondents were allowed to report using as many training types as applicable. “Not Applicable” refers to those organizations that did not implement that type of training in 2021. In addition to the above responses, respondents were able to choose “Other.” Some of those responses included: Active shooter; De-escalation; Crime prevention; AED/CPR training; Behavioral threat assessment; Diversity, equity and inclusion (DEI); Drug diversion awareness; COVID-19 protocols; Zero harm initiative for EHS; Suspicious indicators; Suspicious packages; Taser and firearm; Female travelers; Travel security; and Mental health. SOURCE: The Security Benchmark Report, November 2022

What Does Your Organization Plan to Spend on Electronic Physical Security Systems and Services in 2022?

Respondents report how much they plan to spend on security systems and services by year’s end.

- $1 million or more — 39%
- $500,000 to $999,999 — 20%
- $250,000 to $499,000 — 12%
- $100,000 to $249,000 — 11%
- $50,000 to $99,999 — 7%
- $25,000 to $49,000 — 5%
- Less than $25,000 — 6%

The Security Benchmark Report respondents were asked how much their organization plans to spend on electronic physical security systems and services this year. Respondents were asked to choose the range that best describes their planned spending. SOURCE: The Security Benchmark Report, November 2022
**SECURITY-RELATED TRAINING & TECHNOLOGY**

**What Physical Security / Electronic Security Systems Does Your Enterprise Currently Have in Place?**

Respondents report on which security systems and technologies their organization is using.

<table>
<thead>
<tr>
<th>Security System</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video management system (VMS)</td>
<td>98%</td>
</tr>
<tr>
<td>Access control</td>
<td>96%</td>
</tr>
<tr>
<td>ID / badging</td>
<td>94%</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>83%</td>
</tr>
<tr>
<td>Visitor management systems</td>
<td>82%</td>
</tr>
<tr>
<td>Two-way radio*</td>
<td>81%</td>
</tr>
<tr>
<td>Intercom / communications</td>
<td>80%</td>
</tr>
<tr>
<td>Mass notification</td>
<td>77%</td>
</tr>
<tr>
<td>Perimeter security</td>
<td>65%</td>
</tr>
<tr>
<td>Facility risk monitoring / alert system</td>
<td>60%</td>
</tr>
<tr>
<td>Travel security monitoring</td>
<td>53%</td>
</tr>
<tr>
<td>Executive tracking</td>
<td>31%</td>
</tr>
<tr>
<td>Drones / robots</td>
<td>23%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked which physical and / or electronic security systems and equipment their enterprise currently has in place. Respondents were able to choose as many systems as applicable. Respondents were also allowed to say which "Other" security technologies they have implemented in their enterprises, and some of those include: weather notification; mobile phone incident reporting application; thermal cameras; physical access control systems; K-9 detection; license plate recognition; shooter detection; or duress. *Two-way radio systems are included here if reported for security personnel only. SOURCE: The Security Benchmark Report, November 2022
## SECURITY TEAMS USING METRICS

### Security Teams Emphasizing Metrics to Define Productivity

These security programs report maintaining a metrics program that clearly defines productivity, value creation and cost avoidance.

<table>
<thead>
<tr>
<th>Company</th>
<th>Security Benchmark Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbott</td>
<td>Geoff Shank, Divisional Vice President</td>
</tr>
<tr>
<td>AB InBev</td>
<td>Tom Yarbrough, Head of Global Security</td>
</tr>
<tr>
<td>Actionet</td>
<td>Shelly Nuessle, Information Systems Security Manager</td>
</tr>
<tr>
<td>Adtalem Global Education</td>
<td>Robert Soderberg, Vice President, Chief Safety, Security &amp; Resiliency Officer</td>
</tr>
<tr>
<td>AdventHealth Central Florida Division</td>
<td>Christopher C. Fender, Executive Director of Safety, Security &amp; Emergency Management</td>
</tr>
<tr>
<td>American Electric Power</td>
<td>Steve Swick, Chief Security &amp; Privacy Officer</td>
</tr>
<tr>
<td>American Family Insurance</td>
<td>Vice President, Protective Services</td>
</tr>
<tr>
<td>American Systems Corporation</td>
<td>Dr. Matthew D. Hollandsworth, CISSP, CPP, Director, Corporate Security, Facilities &amp; Safety</td>
</tr>
<tr>
<td>Arthrex</td>
<td>Kevin Cliff, Director, Global Corporate Security</td>
</tr>
<tr>
<td>Associated Grocers of New England Inc.</td>
<td>Alan R. Cote, Director of Risk Management</td>
</tr>
<tr>
<td>AutoZone</td>
<td>Jennie Anderson, Vice President, Loss Prevention &amp; Safety</td>
</tr>
<tr>
<td>AVANGRID</td>
<td>Brian Harrell, Vice President &amp; Chief Security Officer</td>
</tr>
<tr>
<td>Baker Hughes</td>
<td>Kevin Wetherington, Chief Health Safety Environment, Security &amp; Quality Officer</td>
</tr>
<tr>
<td>Ballad Health</td>
<td>Ken Harr, Corporate Director / Chief Security Officer Safety, Security &amp; Emergency Management</td>
</tr>
<tr>
<td>Baycrest Centre for Geriatric Care</td>
<td>Martin Green, Manager, Security, Telecommunications &amp; Emergency Preparedness</td>
</tr>
<tr>
<td>BeiGene</td>
<td>Eric J. Van Balen, Head of Global Security</td>
</tr>
<tr>
<td>Big Lots</td>
<td>Robert LaCommare, CFI, Vice President Asset Protection, Safety, &amp; eCommerce Fraud</td>
</tr>
<tr>
<td>Biogen Inc.</td>
<td>Daniel Biran, Vice President, Global Security</td>
</tr>
<tr>
<td>Black Knight Inc.</td>
<td>Michael A. Skoglund, SVP, Senior Director of Physical Security, Facilities, &amp; IT Asset Management</td>
</tr>
<tr>
<td>Black Knight Security</td>
<td>Dennis W. Lejeck, President</td>
</tr>
<tr>
<td>The Boeing Company</td>
<td>Dave Komendat, Vice President &amp; Chief Security Officer</td>
</tr>
<tr>
<td>Booz Allen Hamilton</td>
<td>Richard M. Lake, Vice President, Security Services</td>
</tr>
<tr>
<td>Boston Children's Hospital</td>
<td>Robert Ryan, Senior Director of Security</td>
</tr>
<tr>
<td>Builders FirstSource</td>
<td>Randy Johnson, Director of Loss Prevention</td>
</tr>
<tr>
<td>Chubb</td>
<td>Richard M. Kelly, Senior Vice President, Chief Security Officer</td>
</tr>
<tr>
<td>CIP Corps</td>
<td>Karl Perman, CEO</td>
</tr>
<tr>
<td>The Claremont Colleges Services Campus Safety Department</td>
<td>Stan Skipworth, Associate Vice President</td>
</tr>
<tr>
<td>Clarios</td>
<td>Robb Koops, Global Security Director</td>
</tr>
<tr>
<td>Cleveland Clinic</td>
<td>Gordon Snow, Chief Security Officer</td>
</tr>
<tr>
<td>Corning Incorporated</td>
<td>Steve Harrold, Vice President, Corporate Security</td>
</tr>
<tr>
<td>Denver Health Medical Center</td>
<td>Eric Smith, Director of Security Services</td>
</tr>
<tr>
<td>Ellis Park Racing &amp; Gaming</td>
<td>Matthew Pressley, Security / Surveillance Manager</td>
</tr>
<tr>
<td>Exact Sciences Corporation</td>
<td>Scott A. Brinkman, Associate Director, Global Corporate Security</td>
</tr>
<tr>
<td>Fidelity Investments - Global Security and Investigations</td>
<td>Craig Magaw, Chief Security Officer</td>
</tr>
<tr>
<td>Franciscan Health Olympia Fields</td>
<td>Daniel Lempa, Director of Safety &amp; Security</td>
</tr>
<tr>
<td>Gap Inc.</td>
<td>Chris Nelson, Senior Vice President, Asset Protection</td>
</tr>
<tr>
<td>GE Healthcare</td>
<td>Shiva Rajagopalan, Senior Director, Security Operations</td>
</tr>
<tr>
<td>Geisinger</td>
<td>Sean McGinley, Associate Vice President, Security Operations</td>
</tr>
<tr>
<td>General Dynamics</td>
<td>Jeffrey Mazaneck, Chief Security Officer</td>
</tr>
<tr>
<td>Global Atlantic Financial Group</td>
<td>Robert Shickel, Senior Vice President, Chief Security &amp; Resilience Officer</td>
</tr>
</tbody>
</table>
### SECURITY TEAMS USING METRICS

#### Security Teams Emphasizing Metrics to Define Productivity - continued

These security programs report maintaining a metrics program that clearly defines productivity, value creation and cost avoidance.

<table>
<thead>
<tr>
<th>Company</th>
<th>Security Benchmark Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>Jason Veiock, Senior Director, Safety, Security &amp; Resilience</td>
</tr>
<tr>
<td>GuideWell</td>
<td>George Frandsen, Senior Director</td>
</tr>
<tr>
<td>Holcim</td>
<td>Cedrick Moriggi, Chief Resilience Officer</td>
</tr>
<tr>
<td>The Jackson Laboratory</td>
<td>Brian O'Rourke, Senior Director, Global Security Services</td>
</tr>
<tr>
<td>Jcshop</td>
<td>Larry Payne, CEO</td>
</tr>
<tr>
<td>Kellogg Company</td>
<td>Scott Lindahl, Vice President, Chief Security Officer</td>
</tr>
<tr>
<td>Kyndryl</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>Massachusetts General Hospital</td>
<td>Bonnie Michelman, Executive Director, Police, Security &amp; Outside Services</td>
</tr>
<tr>
<td>Materion Corporation</td>
<td>Monica N. Mellas, CPP, Vice President</td>
</tr>
<tr>
<td>McKesson Corporation</td>
<td>David Aflalo, Senior Vice President &amp; Chief Security Officer</td>
</tr>
<tr>
<td>McLeod Health</td>
<td>J. Wayne Byrd, Director of Security</td>
</tr>
<tr>
<td>Memorial Healthcare</td>
<td>Jeff Hauk, MSA, CPP, CHPA, PEM, Director, Public Safety &amp; Police Authority Services</td>
</tr>
<tr>
<td>Meta</td>
<td>Nick Lovrien, Chief Global Security Officer</td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>Brian K. Tuskan, Chief Security Officer, Senior Director of Security (Physical)</td>
</tr>
<tr>
<td>Nationwide Mutual</td>
<td>Jay Beighley, Associate Vice President</td>
</tr>
<tr>
<td>News Corp</td>
<td>Eduardo Jany, Chief Security Officer</td>
</tr>
<tr>
<td>NRG</td>
<td>Joe Walters, Senior Director, Enterprise Security &amp; Real Estate</td>
</tr>
<tr>
<td>OEIS Protection Inc.</td>
<td>Ihab Mansour, CEO</td>
</tr>
<tr>
<td>Oracle</td>
<td>Michael Maloof, Vice President</td>
</tr>
<tr>
<td>Orlando City Soccer Club / Exploria Stadium</td>
<td>Robert Schnettler, Senior Director of Security &amp; Guest Services</td>
</tr>
<tr>
<td>Raytheon Technologies</td>
<td>Tammi Morton, Vice President &amp; Chief Security Officer</td>
</tr>
<tr>
<td>San Gorgonio Memorial Hospital</td>
<td>Joey E. Hunter Sr., Director of Security, Safety &amp; Emergency Preparedness</td>
</tr>
<tr>
<td>Scripps Health</td>
<td>Anthony J. Roman, MA-HuB, CPP, CHPA, Corporate Director, Support Operations</td>
</tr>
<tr>
<td>Seattle Children's Hospital</td>
<td>Jim Sawyer, Security Director</td>
</tr>
<tr>
<td>Shanghai Tongtai Information Technology Co. Ltd.</td>
<td>Xuehui Hu, CIO</td>
</tr>
<tr>
<td>Sparrow Hospital</td>
<td>Jerry Dumond, Director of Public Safety, Chief of Police</td>
</tr>
<tr>
<td>State Street Corporation</td>
<td>Stephen D. Baker, CPP, Senior Vice President &amp; Chief Security Officer</td>
</tr>
<tr>
<td>Synopsys Inc.</td>
<td>Jim Fussell, Senior Director, Global Safety &amp; Security</td>
</tr>
<tr>
<td>Takeda Pharmaceuticals Company Ltd</td>
<td>Whit Chaiyabhat, Vice President, Head of Global Security &amp; Crisis Management</td>
</tr>
<tr>
<td>Texas Biomedical Research Institute</td>
<td>Mark A. Hammargren, CPP, Director, Security &amp; Emergency Preparedness</td>
</tr>
<tr>
<td>Thrivent</td>
<td>Mark Theisen, Director, Corporate Security &amp; Business Resilience</td>
</tr>
<tr>
<td>United Therapeutics Corporation</td>
<td>Michael W. Wanik, Senior Director, Corporate Security</td>
</tr>
<tr>
<td>University Health Network</td>
<td>Todd Milne, Director, Security Operations, UHN CONNECT, Fire &amp; Life Safety</td>
</tr>
<tr>
<td>University of Alabama at Birmingham</td>
<td>Anthony Purcell, Associate Vice President, Public Safety &amp; Chief of Police</td>
</tr>
<tr>
<td>University of Pennsylvania</td>
<td>Kathleen Shields Anderson, J.D., MBA, Vice President for Public Safety</td>
</tr>
<tr>
<td>VF Corporation</td>
<td>Justin Cullinan, Vice President for Public Safety</td>
</tr>
<tr>
<td>Victoria's Secret &amp; Co</td>
<td>John Talamo, Senior Vice President - Asset Protection</td>
</tr>
<tr>
<td>Wellstar Health System</td>
<td>Adrian Arriaga, Executive Director of Security</td>
</tr>
<tr>
<td>Whirlpool Corporation</td>
<td>Erik Antons, Chief Security Officer</td>
</tr>
<tr>
<td>Wolfpack Protective Services Inc.</td>
<td>Justin Joyce, CEO</td>
</tr>
</tbody>
</table>

The above list (in alphabetical order) are those security leaders that reported maintaining a security metrics program that defines productivity, value creation and cost avoidance. Respondents are allowed to remain anonymous from any listings or rankings within the published The Security Benchmark Report; therefore, any respondents choosing to remain anonymous are not included in this list. SOURCE: The Security Benchmark Report, November 2022
Among the Security Benchmark Report respondents choosing Aerospace & Defense as their primary market sector, 2.1% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

The Security Benchmark Report respondents in the Aerospace & Defense sector reported an average of $133,000 in security-related spending last year. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
AEROSPACE & DEFENSE

Security Budget 2022 vs. 2021 — Aerospace & Defense

<table>
<thead>
<tr>
<th>Budget Change</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased</td>
<td>40%</td>
</tr>
<tr>
<td>Stayed the Same</td>
<td>40%</td>
</tr>
<tr>
<td>Decreased</td>
<td>20%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents in the Aerospace & Defense sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. SOURCE: The Security Benchmark Report, November 2022

5 Responsibilities Owned by Aerospace & Defense Security Teams

1. Aligning security with the business
2. Security staff development & training
3. Security strategy
4. Terrorism / extremism
5. Workplace violence / active shooter prevention

The Security Benchmark Report respondents within the Aerospace & Defense sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities (in alphabetical order) that the security function within this sector reported as Owning / Leading. For this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Aerospace & Defense

Respondents in this sector report which function security reports to or resides within.

<table>
<thead>
<tr>
<th>Function</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAO / Administration</td>
<td>40%</td>
</tr>
<tr>
<td>CFO / Finance</td>
<td>20%</td>
</tr>
<tr>
<td>COO / Operations</td>
<td>20%</td>
</tr>
<tr>
<td>Human Resources</td>
<td>20%</td>
</tr>
</tbody>
</table>

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Aerospace & Defense sector, the highest percentage of security teams reported to Administration. SOURCE: The Security Benchmark Report, November 2022

Structure of Security — Aerospace & Defense

<table>
<thead>
<tr>
<th>Structure Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>60%</td>
</tr>
<tr>
<td>Decentralized</td>
<td>40%</td>
</tr>
</tbody>
</table>

In the Aerospace & Defense sector, 60% of Security Benchmark Report respondents reported a Centralized structure of their security organization. Zero respondents in this sector chose Regional. SOURCE: The Security Benchmark Report, November 2022
Who’s responsible for both physical security and cybersecurity?

40% of Aerospace & Defense security leaders reported being responsible for both physical security and cybersecurity.

Who’s responsible for both physical security and health & safety?

20% of Aerospace & Defense security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Aerospace & Defense

Respondents report which geographic areas they provide risk and security services to.

North America — 100%
Europe — 100%
Asia — 100%
Africa — 80%
Oceania (including Australia) — 80%
South America — 80%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Aerospace & Defense sector, 80% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022.
Among The Security Benchmark Report respondents choosing Agriculture, Food & Beverage or Construction as their primary sector, 4.9% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation.

SOURCE: The Security Benchmark Report, November 2022

Among The Security Benchmark Report respondents choosing Agriculture, Food & Beverage and Construction sectors as their primary sector, the average security budget as a percent of total revenue was 4.9%.

Among The Security Benchmark Report respondents choosing Agriculture, Food & Beverage and Construction sectors as their primary market sector of business, the average amount of money spent on security-related training in 2021 was $68,750.

The Security Benchmark Report respondents in the Agriculture, Food & Beverage and Construction sectors reported an average of $68,750 in security-related spending last year. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
Security Budget 2022 vs. 2021 — Agriculture, Food & Beverage, Construction

Stayed the Same — **67%**

Increased — **33%**

The Security Benchmark Report respondents in the Agriculture, Food & Beverage and Construction sectors were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. Zero percent of respondents in this sector reported a decrease in security budget. SOURCE: The Security Benchmark Report, November 2022

5 Responsibilities Owned by Agriculture, Food & Beverage and Construction Security Teams

1. Aligning security with the business
2. Liaison with public sector / law enforcement agencies
3. Security audits, surveys, assessments
4. Security strategy
5. Terrorism / extremism

The Security Benchmark Report participants within the Agriculture, Food & Beverage and Construction sectors were given a list of 37 roles and responsibilities that may fall under the security function at an organization and were asked for the level of responsibility the team has over that role within their enterprise. These (in alphabetical order) are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Agriculture, Food & Beverage, Construction

Respondents report which function security reports to or resides within.

CRO / Risk / Legal / General Counsel — **50%**

COO / Operations — **33%**

CFO / Finance — **17%**

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Agriculture, Food & Beverage and Construction sectors, the highest percentage of security teams reported to CRO / Risk / Legal / General Counsel. SOURCE: The Security Benchmark Report, November 2022

Structure of Security — Agriculture, Food & Beverage, Construction

Centralized — **66%**

Decentralized — **17%**

Regional — **17%**

In the Agriculture, Food & Beverage and Construction sectors, 66% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another. SOURCE: The Security Benchmark Report, November 2022
AGRICULTURE, FOOD & BEVERAGE, CONSTRUCTION

Who’s responsible for both physical security and cybersecurity?

0% of Agriculture, Food & Beverage and Construction security leaders reported being responsible for both physical security and cybersecurity.

Who’s responsible for both physical security and health & safety?

0% of Agriculture, Food & Beverage and Construction security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Agriculture, Food & Beverage, Construction

Respondents report which geographic areas they provide risk and security services to.

North America — 100%

Europe — 83%

South America — 83%

Asia — 83%

Oceania (including Australia) — 67%

Africa — 67%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Agriculture, Food & Beverage and Construction sectors, 33% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. 

**Source:** The Security Benchmark Report, November 2022

---

**Guarding Insights — Agriculture, Food & Beverage, Construction**

- **3,299** Average number of enterprise-wide contract FTE security officers / guards within Agriculture, Food & Beverage and Construction sector organizations.

- **92** Average number of enterprise-wide proprietary FTE security officers / guards within Agriculture, Food & Beverage and Construction sector organizations.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Agriculture, Food & Beverage and Construction sectors is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. 

**Source:** The Security Benchmark Report, November 2022
Among The Security Benchmark Report respondents choosing Banking & Insurance as their primary sector, 0.3% was the average security budget as a percent of revenue. To calculate the security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. 

**SOURCE:** The Security Benchmark Report, November 2022

0.3% Security Budget as a Percent of Revenue — Banking & Insurance

Among The Security Benchmark Report respondents choosing Banking & Insurance as their primary sector, 0.3% was the average security budget as a percent of revenue. To calculate the security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. **SOURCE:** The Security Benchmark Report, November 2022

Money Spent on Security-Related Training — Banking & Insurance

Among the Banking & Insurance sector, the **average amount of money spent on security-related training** in 2021 was $76,000.

The Security Benchmark Report respondents in the Banking & Insurance sector reported an average of $76,000 in security-related spending last year. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. **SOURCE:** The Security Benchmark Report, November 2022
The Security Benchmark Report respondents in the Banking & Insurance sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. SOURCE: The Security Benchmark Report, November 2022

Security Budget 2022 vs. 2021 — Banking & Insurance

<table>
<thead>
<tr>
<th>Increased</th>
<th>58%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decreased</td>
<td>25%</td>
</tr>
<tr>
<td>Stayed the Same</td>
<td>17%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report participants within the Banking & Insurance sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

8 Responsibilities Owned by Banking & Insurance Security Teams

1. Asset protection / facilities protection
2. Event security
3. Liaison with public sector / law enforcement agencies
4. Security strategy
5. Security technology & integration
6. Targeted protests / activists / hate crimes
7. Terrorism / extremism
8. Workplace violence / active shooter prevention

Where Security Lives — Banking & Insurance

Respondents within this sector report where security reports to or resides within.

<table>
<thead>
<tr>
<th>CRO / Risk / Legal / General Counsel</th>
<th>43%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>25%</td>
</tr>
<tr>
<td>Board or Board Committee</td>
<td>8%</td>
</tr>
<tr>
<td>CAO / Administration / Shared Services</td>
<td>8%</td>
</tr>
<tr>
<td>CFO / Finance</td>
<td>8%</td>
</tr>
<tr>
<td>Facilities</td>
<td>8%</td>
</tr>
</tbody>
</table>

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Banking & Insurance sector, the highest percentage of security teams reported to CRO / Risk / Legal / General Counsel. SOURCE: The Security Benchmark Report, November 2022
BANKING & INSURANCE

Structure of Security — Banking & Insurance

100% Centralized

In the Banking & Insurance sectors, 100% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. SOURCE: The Security Benchmark Report, November 2022

Who's responsible for both physical security and cybersecurity?

8% of Banking & Insurance security leaders reported being responsible for both physical security and cybersecurity.

Who's responsible for both physical security and health & safety?

58% of Banking & Insurance security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Banking & Insurance

Respondents report which geographic areas their security organization provides risk and security services to.

North America — 100%
Asia — 58%
Europe — 50%
Oceania (including Australia) — 33%
South America — 33%
Africa — 33%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Banking & Insurance sector, 92% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Do Banking & Insurance Organizations Have Security Operations Centers?

- **YES 92%**
- **NO 8%**

Guarding Insights — Banking & Insurance

- **142** Average number of enterprise-wide contract FTE security officers / guards within Banking & Insurance sector organizations.
- **28** Average number of enterprise-wide proprietary FTE security officers / guards within Banking & Insurance sector organizations.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers and guards they have within their enterprise. The average among all respondents in the Banking & Insurance sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
Among The Security Benchmark Report respondents choosing Business Services & Consulting as their primary sector, 4% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. 

**SOURCE:** The Security Benchmark Report, November 2022

---

Among the Business Services & Consulting sector, the **average security budget as a percent of total revenue** was 4%.

---

The Security Benchmark Report respondents in the Business Services & Consulting sector reported an average of $54,500 in security-related spending last year. Information that appeared to be inaccurately reported was excluded from the calculation.

**SOURCE:** The Security Benchmark Report, November 2022
BUSINESS SERVICES & CONSULTING

**Security Budget 2022 vs. 2021 — Business Services & Consulting**

Increased — **83%**

Stayed the Same — **17%**

The Security Benchmark Report respondents in the Business Services & Consulting sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. Zero percent of respondents in this sector reported a decrease in security budget. SOURCE: The Security Benchmark Report, November 2022

<table>
<thead>
<tr>
<th>10 Responsibilities Owned by Business Services &amp; Consulting Security Teams</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Aligning security with the business</td>
</tr>
<tr>
<td>2. Asset protection / facilities protection</td>
</tr>
<tr>
<td>3. Business expansion support</td>
</tr>
<tr>
<td>4. Business resilience</td>
</tr>
<tr>
<td>5. Investigations</td>
</tr>
<tr>
<td>6. Liaison with public sector / law enforcement agencies</td>
</tr>
<tr>
<td>7. Risk / threat assessments / risk management planning / enterprise risk management</td>
</tr>
<tr>
<td>8. Security audits / surveys / assessments</td>
</tr>
<tr>
<td>9. Security strategy</td>
</tr>
<tr>
<td>10. Workplace violence / active shooter prevention</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents within the Business Services & Consulting sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These (in alphabetical order) are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

**Where Security Lives — Business Services & Consulting**

Respondents in this sector report which function security reports to or resides within.

CEO / President / Owner / Exec. Director — **66%**

Board or Board Committee — **17%**

CFO / Finance — **17%**

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Business Services & Consulting market sector, the highest percentage of security teams reported to the CEO, President, Owner or Executive Director. SOURCE: The Security Benchmark Report, November 2022
In the Business Services & Consulting sector, 66% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another. SOURCE: The Security Benchmark Report, November 2022

**Structure of Security — Business Services & Consulting**

- Centralized — 66%
- Decentralized — 17%
- Regional — 17%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services to. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022

**Geographic Security Responsibility — Business Services & Consulting**

Respondents report which geographic areas they provide risk and security services to.

- North America — 100%
- Europe — 33%
- Asia — 17%

In the Business Services & Consulting sector, 50% of The Security Benchmark Report respondents reported being responsible for both physical security and cybersecurity.

SOURCE: The Security Benchmark Report, November 2022

50% of Business Services & Consulting security leaders reported being responsible for both physical security and cybersecurity.

SOURCE: The Security Benchmark Report, November 2022

67% of Business Services & Consulting security leaders reported being responsible for both physical security and health & safety.

SOURCE: The Security Benchmark Report, November 2022

Who’s responsible for both physical security and cybersecurity?

Who’s responsible for both physical security and health & safety?
Within the Business Services & Consulting sector, 50% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Do Business Services & Consulting Organizations Have Security Operations Centers?

- **NO** 50%
- **YES** 50%

Guarding Insights — Business Services & Consulting

- **108** Average number of enterprise-wide **contract** FTE security officers / guards within Business Services & Consulting sector organizations.
- **0** Average number of enterprise-wide **proprietary** FTE security officers / guards within Business Services & Consulting sector organizations.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers and guards they have within their enterprise. The average among all respondents in the Business Services & Consulting sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
ENTERTAINMENT & CULTURAL INSTITUTIONS

This sector includes those organizations reporting entertainment (sports leagues, media & publishing, TV, movies, video, gaming, recreation, amusement parks, sports facilities) or cultural institutions (museums, gardens, zoos, etc.) as their primary market sector of business.

Security Budget as a Percent of Revenue — Entertainment & Cultural Institutions

Among the Entertainment & Cultural Institution sectors, the average security budget as a percent of total revenue was 3.4%.

Money Spent on Security-Related Training — Entertainment & Cultural Institutions

Among the Entertainment & Cultural Institution sectors, the average amount of money spent on security-related training in 2021 was $25,500.

The Security Benchmark Report respondents in the Entertainment & Cultural Institution sectors reported an average of $25,500 in security-related spending last year. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
ENTERTAINMENT & CULTURAL INSTITUTIONS

Security Budget 2022 vs. 2021 — Entertainment & Cultural Institutions

Increased — **86%**

Stayed the Same — **14%**

The Security Benchmark Report respondents in the Entertainment & Cultural Institution sectors asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. Zero respondents in this sector reported a security budget decrease over last year. **SOURCE:** The Security Benchmark Report, November 2022

10 Responsibilities *Owned* by Entertainment & Cultural Institution Security Teams

1. Asset protection / facilities protection
2. Business resilience
3. Civil unrest / disturbances / riots
4. Emergency notification
5. Emergency response planning
6. Event security
7. Risk / threat assessments / risk management planning / enterprise risk management
8. Security operations center management
9. Security staff development & training
10. Weather / natural disasters

The Security Benchmark Report participants within the Entertainment & Cultural Institution sectors were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. **SOURCE:** The Security Benchmark Report, November 2022

Where Security Lives — Entertainment & Cultural Institutions

Respondents report which function security reports to or resides within.

- CRO / Risk / Legal / General Counsel — **29%**
- General Manager / Business Unit — **29%**
- CAO / Administration / Shared Services — **14%**
- CEO / President / Owner / Exec. Director — **14%**
- Human Resources — **14%**

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Entertainment & Cultural Institution sectors, an even split of security teams reported to General Manager or CRO / Risk / Legal / General Counsel. **SOURCE:** The Security Benchmark Report, November 2022
In the Entertainment & Cultural Institution sectors, 57% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another.

SOURCE: The Security Benchmark Report, November 2022

In the Entertainment & Cultural Institution sectors, 57% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another.

SOURCE: The Security Benchmark Report, November 2022

Who’s responsible for both physical security and cybersecurity?

29% of Entertainment & Cultural Institution security leaders reported being responsible for both physical security and cybersecurity.

Who’s responsible for both physical security and health & safety?

71% of Entertainment & Cultural Institution security leaders reported being responsible for both physical security and health & safety.

SOURCE: The Security Benchmark Report, November 2022

Geographic Security Responsibility — Entertainment & Cultural Institutions

Respondents report which geographic areas they provide risk and security services to.

North America — 100%

Africa — 33%

Asia — 33%

Europe — 33%

Oceania (including Australia) — 33%

South America — 33%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
### Do Entertainment & Cultural Institutions Have Security Operations Centers?

**Yes** 100%

Within the Entertainment & Cultural Institution sectors, 100% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. *SOURCE: The Security Benchmark Report, November 2022*

### Guarding Insights — Entertainment & Cultural Institutions

<table>
<thead>
<tr>
<th></th>
<th>Average number of enterprise-wide contract FTE security officers / guards within Entertainment &amp; Cultural Institutions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>31</strong></td>
<td></td>
</tr>
<tr>
<td><strong>20</strong></td>
<td>Average number of enterprise-wide proprietary FTE security officers / guards within Entertainment &amp; Cultural Institutions.</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Entertainment & Cultural Institution sectors is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. *SOURCE: The Security Benchmark Report, November 2022*
Among The Security Benchmark Report respondents choosing Healthcare as their primary market sector, 3.1% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Outliers or information that appeared to be inaccurately reported were excluded from the calculation.

SOURCE: The Security Benchmark Report, November 2022

Among the Healthcare sector, the average security budget as a percent of total revenue was 3.1%.

Security Budget as a Percent of Revenue — Healthcare

$208,800

Among The Security Benchmark Report respondents choosing Healthcare as their primary market sector, 37% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

Money Spent on Security-Related Training — Healthcare

The Security Benchmark Report respondents in the Healthcare sector reported an average of $208,800 in security-related spending last year. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
HEALTHCARE

Security Budget 2022 vs. 2021 — Healthcare

Increased — 74%
Decreased — 17%
Stayed the Same — 9%

The Security Benchmark Report respondents in the Healthcare sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. The majority of respondents reported an increase in security budget over last year, with the average percent increase being 16%. SOURCE: The Security Benchmark Report, November 2022

8 Responsibilities Owned by Healthcare Security Teams

1. Asset protection / facilities protection
2. Liaison with public sector / law enforcement agencies
3. Loss prevention / goods protection
4. Security operations center management
5. Security staff development & training
6. Security strategy
7. Terrorism / extremism
8. Workplace violence / active shooter prevention

The Security Benchmark Report participants within the Healthcare sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Healthcare

Respondents in this sector report which function security reports to or resides within.

COO / Operations — 35%
CRO / Risk / Legal / General Counsel — 22%
CAO / Administration / Shared Services — 18%
Other — 13%
CFO / Finance — 4%
Facilities — 4%
Human Resources — 4%

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Healthcare sector, the majority of security functions reported to or resided within Operations. SOURCE: The Security Benchmark Report, November 2022
HEALTHCARE

Structure of Security — Healthcare

Centralized — 74%
Decentralized — 13%
Regional — 13%

In the Healthcare sector, 74% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another. SOURCE: The Security Benchmark Report, November 2022

Who's responsible for both physical security and cybersecurity?

9% of Healthcare security leaders reported being responsible for both physical security and cybersecurity.

Who's responsible for both physical security and health & safety?

52% of Healthcare security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Healthcare

Respondents report which geographic areas they provide risk and security services to.

North America — 100%
Asia — 13%
Europe — 13%
South America — 9%
Africa — 4%
Oceania (including Australia) — 4%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Healthcare sector, 61% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Guarding Insights — Healthcare

| 49 | Average number of enterprise-wide contract FTE security officers / guards within the Healthcare sector. |
| 110 | Average number of enterprise-wide proprietary FTE security officers / guards within the Healthcare sector. |

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Healthcare sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
Among the Higher Education sector, the average security budget as a percent of total revenue was 1.9%.

Among The Security Benchmark Report respondents choosing Higher Education as their primary sector, 19% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

Among the Higher Education sector, the average amount of money spent on security-related training in 2021 was $16,500.

The Security Benchmark Report respondents in the Higher Education sector reported an average of $16,500 in security-related spending last year. Outliers or information appearing to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
The Security Benchmark Report respondents in the Higher Education sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. All respondents in this sector reported a security budget increase over last year, with an average budget increase of 9.3%. SOURCE: The Security Benchmark Report, November 2022

Security Budget 2022 vs. 2021 — Higher Education

| Increased | 100% |

The Security Benchmark Report participants within the Higher Education sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

8 Responsibilities Owned by Higher Education Security Teams

1. Asset protection / facilities protection
2. Civil unrest / disturbances / riots
3. Liaison with public sector / law enforcement agencies
4. Security operations center management
5. Security strategy
6. Targeted protests / activists / hate crimes
7. Terrorism / extremism
8. Workplace violence / active shooter prevention

The Security Benchmark Report participants within the Higher Education sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Higher Education

Respondents in this sector report which function security reports to or resides within.

| CEO / President / Owner / Executive Director — 33% |
| COO / Operations — 33% |
| CFO / Finance — 17% |
| CAO / Administration / Shared Services — 17% |

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Higher Education sector, an even split of security teams reported to Operations and President/Executive Director. SOURCE: The Security Benchmark Report, November 2022
In the Higher Education sector, 83% of The Security Benchmark Report respondents reported a Centralized structure of their security organization.

SOURCE: The Security Benchmark Report, November 2022

<table>
<thead>
<tr>
<th>Structure of Security — Higher Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized — 83%</td>
</tr>
<tr>
<td>Partially Centralized &amp; Partially Decentralized — 17%</td>
</tr>
</tbody>
</table>

Who's responsible for both physical security and cyber security?

0% of Higher Education security leaders reported being responsible for both physical security and cybersecurity.

Who's responsible for both physical security and health & safety?

33% of Higher Education security leaders reported being responsible for both physical security and health & safety.

SOURCE: The Security Benchmark Report, November 2022

Geographic Security Responsibility — Higher Education
Respondents report which geographic areas they provide risk and security services to.

<table>
<thead>
<tr>
<th>Geographic Area</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>100%</td>
</tr>
<tr>
<td>Asia</td>
<td>50%</td>
</tr>
<tr>
<td>Africa</td>
<td>33%</td>
</tr>
<tr>
<td>Europe</td>
<td>33%</td>
</tr>
<tr>
<td>Oceania (including Australia)</td>
<td>33%</td>
</tr>
<tr>
<td>South America</td>
<td>33%</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Higher Education sector, 83% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Do Higher Education Organizations Have Security Operations Centers?

- **NO 17%**
- **YES 83%**

Guarding Insights — Higher Education

- **163** Average number of enterprise-wide contract FTE security officers / guards within Higher Education organizations.
- **39** Average number of enterprise-wide proprietary FTE security officers / guards within Higher Education organizations.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Higher Education sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
Among the Security Benchmark Report respondents choosing Information Technology & Media as their primary sector, 0.4% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

Among the Information Technology & Media sector, the average security budget as a percent of total revenue was 0.4%.

The Security Benchmark Report respondents in the Information Technology & Media sector reported an average of $72,600 in security-related spending last year. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

Among the Information Technology & Media sector, the average amount of money spent on security-related training in 2021 was $72,600.
The Security Benchmark Report respondents in the Information Technology & Media sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. The majority of respondents reported an increase in security budget over last year, with the average percent increase being 20%. SOURCE: The Security Benchmark Report, November 2022

Security Budget 2022 vs. 2021 — Information Technology & Media

Increased — 67%
Stayed the Same — 33%

The Security Benchmark Report participants within the Information Technology & Media sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

7 Responsibilities Owned by Information Technology & Media Security Teams

1. Emergency notification
2. Emergency response & planning
3. Liaison with public sector / law enforcement agencies
4. Security operations center management
5. Security staff development & training
6. Security strategy
7. Workplace violence / active shooter prevention

Where Security Lives — Information Technology & Media

Respondents in this sector report which function security reports to or resides within.

CIO / Information Technology — 25%
CFO / Finance — 25%
CEO / President / Owner / Executive Director — 18%
Board or Board Committee — 8%
CRO / Risk / Legal / General Counsel — 8%
Facilities — 8%
Human Resources — 8%

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Information Technology & Media sector, the majority of security functions reported to or resided within Information Technology or Finance. SOURCE: The Security Benchmark Report, November 2022
INFORMATION TECHNOLOGY & MEDIA

Structure of Security — Information Technology & Media

Centralized — 92%

Partially Centralized & Partially Decentralized — 8%

In the Information Technology & Media sector, 92% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. Zero respondents within this sector reported a Regional structure. SOURCE: The Security Benchmark Report, November 2022

Who's responsible for both physical security and cybersecurity?

42% of Information Technology & Media security leaders reported being responsible for both physical security and cybersecurity.

Who's responsible for both physical security and health & safety?

58% of Information Technology & Media security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Information Technology & Media

Respondents report which geographic areas they provide risk and security services to.

North America — 83%

Asia — 75%

Europe — 67%

Oceania (including Australia) — 67%

Africa — 58%

South America — 58%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Information Technology & Media sector, 58% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Do Information Technology & Media Organizations Have Security Operations Centers?

- **NO** 42%
- **YES** 58%

Guarding Insights — Information Technology & Media

<table>
<thead>
<tr>
<th>390</th>
<th>Average number of enterprise-wide contract FTE security officers / guards within the Information Technology &amp; Media sector.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Average number of enterprise-wide proprietary FTE security officers / guards within the Information Technology &amp; Media sector.</td>
</tr>
</tbody>
</table>

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Information Technology & Media sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
MANUFACTURING

This sector includes those organizations reporting manufacturing as their primary market sector of business.

**Security Budget as a Percent of Revenue — Manufacturing**

Among the Manufacturing sector, the average security budget as a percent of total revenue was 0.5%.

**Money Spent on Security-Related Training — Manufacturing**

Among the Manufacturing sector, the average amount of money spent on security-related training in 2021 was $162,500.
MANUFACTURING

Security Budget 2022 vs. 2021 — Manufacturing

Increased — **72%**

Decreased — **14%**

Stayed the Same — **14%**

The Security Benchmark Report respondents in the Manufacturing sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. The majority of respondents in this sector reported an increase over last year with an average security budget increase of 8%. SOURCE: The Security Benchmark Report, November 2022

10 Responsibilities *Owned* by Manufacturing Teams

1. Aligning security with the business
2. International workforce protection & support
3. Loss prevention / goods protection
4. Security audits / surveys / assessments
5. Security contract management
6. Security operations center management
7. Security staff development & training
8. Security strategy
9. Targeted protests / activists / hate crimes
10. Workplace violence / active shooter prevention

The Security Benchmark Report participants within the Manufacturing sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Manufacturing

Respondents in this sector report which function security reports to or resides within.

- CRO / Risk / Legal / General Counsel — **44%**
- CAO / Administration / Shared Services — **14%**
- CEO / President / Owner / Exec. Director — **14%**
- COO / Operations — **14%**
- Human Resources — **14%**

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. In the Manufacturing sector, 44% of respondents reported to the CRO / Risk / Legal / General Counsel. SOURCE: The Security Benchmark Report, November 2022
MANUFACTURING

Structure of Security — Manufacturing

- Centralized — 58%
- Decentralized — 14%
- Regional — 14%
- Other — 14%

In the Manufacturing sector, 58% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. For this survey’s purpose, the distinction between Decentralized and Regional security is that some Regional security programs may behave in a centralized manner for their determined region, while Decentralized generally means there may be security organizations in multiple locations within an enterprise functioning independently from one another. Respondents choosing Other in this sector reported a functionally Centralized structure with dotted line regional security managers. SOURCE: The Security Benchmark Report, November 2022

Who’s responsible for both physical security and cybersecurity?

0% of Manufacturing security leaders reported being responsible for both physical security and cybersecurity.

Who’s responsible for both physical security and health & safety?

0% of Manufacturing security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Manufacturing

Respondents report which geographic areas they provide risk and security services to.

- Asia — 100%
- Europe — 100%
- North America — 100%
- South America — 86%
- Africa — 71%
- Oceania (including Australia) — 71%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Manufacturing sector, 71% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Do Manufacturing Organizations Have Security Operations Centers?

- **NO 29%**
- **YES 71%**

Guarding Insights — Manufacturing

**313**
Average number of enterprise-wide contract FTE security officers / guards within the Manufacturing sector.

**45**
Average number of enterprise-wide proprietary FTE security officers / guards within the Manufacturing sector.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Manufacturing sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
PHARMA & BIOTECH
This sector includes those organizations reporting pharmaceuticals or biotechnology as their primary market sector of business.

Security Budget as a Percent of Revenue — Pharma & Biotech

Among the Pharma & Biotech sector, the average security budget as a percent of total revenue was 0.5%.

The Security Benchmark Report respondents choosing Pharma & Biotech as their primary sector reported an average of $59,300 in security-related spending last year. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

Money Spent on Security-Related Training — Pharma & Biotech

Among the Pharma & Biotech sector, the average amount of money spent on security-related training in 2021 was $59,300.

The Security Benchmark Report respondents in the Pharma & Biotech sector reported an average of $59,300 in security-related spending last year. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
PHARMA & BIOTECH

Security Budget 2022 vs. 2021 — Pharma & Biotech

Increased — **70%**

Stayed the Same — **30%**

The Security Benchmark Report respondents in the Pharma & Biotech sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. The majority of respondents in this sector reported an increase over last year with an average security budget increase of 15%. Zero respondents in this sector reported a decrease in the security budget compared to last year. SOURCE: The Security Benchmark Report, November 2022

7 Responsibilities Owned by Pharma & Biotech Security Teams

1. Asset protection / facilities protection
2. Duty of care / traveler protection & support
3. Emergency notification
4. Security contract management
5. Security staff development & training
6. Security strategy
7. Workplace violence / active shooter prevention

The Security Benchmark Report participants within the Pharma & Biotech sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Pharma & Biotech

Respondents in this sector report which function security reports to or resides within.

COO / Operations — **40%**

Other — **20%**

CAO / Administration / Shared Services — **10%**

CEO / President / Owner / Exec. Director — **10%**

Facilities — **10%**

Human Resources — **10%**

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. In this sector, those reporting Other included Head of Pharmaceutical Operations and Technology, Chief Global Corporate Affairs and Sustainability Officer. SOURCE: The Security Benchmark Report, November 2022
PHARMA & BIOTECH

Structure of Security — Pharma & Biotech

Centralized — 90%

Other — 10%

In the Pharma & Biotech sector, 90% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. Respondents choosing Other in this sector reported a centralized corporate global security team with decentralized business unit security. SOURCE: The Security Benchmark Report, November 2022

Who’s responsible for both physical security and cybersecurity?

10% of Pharma & Biotech security leaders reported being responsible for both physical security and cybersecurity.

Who’s responsible for both physical security and health & safety?

10% of Pharma & Biotech security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Pharma & Biotech

Respondents report which geographic areas they provide risk and security services to.

North America — 100%

Europe — 90%

Oceania (including Australia) — 90%

Asia — 70%

South America — 70%

Africa — 50%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Pharma & Biotech sector, 80% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Guarding Insights — Pharma & Biotech

- Average number of enterprise-wide contract FTE security officers / guards within the Pharma & Biotech sector: 65
- Average number of enterprise-wide proprietary FTE security officers / guards within the Pharma & Biotech sector: 10

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Pharma & Biotech sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
Among the Retail & Restaurant sector, the average security budget as a percent of total revenue was 1.8%.

Money Spent on Security-Related Training — Retail & Restaurant

Among the Retail & Restaurant sector, the average amount of money spent on security-related training in 2021 was $190,000.
RETAIL & RESTAURANT

Security Budget 2022 vs. 2021 — Retail & Restaurant

Increased — 75%
Stayed the Same — 25%

The Security Benchmark Report respondents in the Retail & Restaurant sector were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. The majority of respondents in this sector reported an increase over last year with an average security budget increase of 8%. Zero respondents in this sector reported a decrease in the security budget compared to last year. SOURCE: The Security Benchmark Report, November 2022

10 Responsibilities Owned by Retail & Restaurant Security Teams

| 1.  | Aligning security with the business |
| 2.  | Asset protection / facilities protection |
| 3.  | Civil unrest / disturbances / riots |
| 4.  | Event security |
| 5.  | Investigations |
| 6.  | Liaison with public sector / law enforcement agencies |
| 7.  | Security operations center management |
| 8.  | Security staff development & training |
| 9.  | Security strategy |
| 10. | Workplace violence / active shooter prevention |

The Security Benchmark Report participants within the Retail & Restaurant sector were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

Where Security Lives — Retail & Restaurant

Respondents in this sector report which function security reports to or resides within.

COO / Operations — 25%
CRO / Risk / Legal / General Counsel — 25%
CEO / President / Owner / Exec. Director — 12.5%
CFO / Finance — 12.5%
Facilities — 12.5%
Human Resources — 12.5%

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. Within the Retail & Restaurant sector, 25% of security teams reported to Operations, while another 25% reported to CRO / Risk / Legal / General Counsel. SOURCE: The Security Benchmark Report, November 2022
In the Retail & Restaurant sector, 100% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. SOURCE: The Security Benchmark Report, November 2022

**Structure of Security — Retail & Restaurant**

- **100%** Centralized

Who's responsible for both physical security and cybersecurity?

- **25%** of Retail & Restaurant security leaders reported being responsible for both physical security and cybersecurity.

Who's responsible for both physical security and health & safety?

- **50%** of Retail & Restaurant security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Retail & Restaurant

Respondents report which geographic areas they provide risk and security services to.

- North America — **100%**
- Asia — **63%**
- Europe — **63%**
- South America — **38%**
- Africa — **13%**
- Oceania (including Australia) — **13%**

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Retail & Restaurant sector, 75% of Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Do Retail & Restaurant Organizations Have Security Operations Centers?

- **YES 75%**
- **NO 25%**

Guarding Insights — Retail & Restaurant

- **102** Average number of enterprise-wide contract FTE security officers / guards within the Retail & Restaurant sector.
- **67** Average number of enterprise-wide proprietary FTE security officers / guards within the Retail & Restaurant sector.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Retail & Restaurant sector is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
Among the Utilities & Distribution sectors, the average security budget as a percent of total revenue was 0.1%. This sector includes those organizations reporting utilities (oil & gas, waste management & equipment, renewable/clean energy, electric, gas, nuclear, wind, environmental services), logistics, warehousing, ports (air, sea, etc.), distribution, shipping or freight transportation as their primary market sector of business.

Among The Security Benchmark Report respondents choosing Utilities or Distribution as their primary sector, 0.1% was the average security budget as a percent of revenue. To calculate security budget as a percentage of revenue across security programs in this sector, the security budget was divided by the total revenue, based on self-reported information. Information that appeared to be inaccurately reported was excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022

Among the Utilities & Distribution sectors, the average amount of money spent on security-related training in 2021 was $60,000. The Security Benchmark Report respondents in the Utilities & Distribution sectors reported an average of $60,000 in security-related spending last year. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
The Security Benchmark Report respondents in the Utilities & Distribution sectors were asked whether their 2022 security budgets increased, decreased or stayed the same over 2021. The majority of respondents reported an increase or the same security budget over last year. SOURCE: The Security Benchmark Report, November 2022

Security Budget 2022 vs. 2021 — Utilities & Distribution

- Increased — **40%**
- Stayed the Same — **40%**
- Decreased — **20%**

The Security Benchmark Report participants within the Utilities & Distribution sectors were given a list of 37 roles and responsibilities that may fall under the security function at an organization, and were asked for the level of responsibility the team has over that role within their enterprise. These are the most common job responsibilities that the security function within this sector reported as Owning / Leading. For the purposes of this survey, Owning / Leading the responsibility means security both manages and funds the program. SOURCE: The Security Benchmark Report, November 2022

9 Responsibilities Owned by Utilities & Distribution Security Teams

1. Aligning security with the business
2. Asset protection / facilities protection
3. Civil unrest / disturbances / riots
4. Event security
5. Liaison with public sector / law enforcement agencies
6. Security audits / surveys / assessments
7. Security staff development & training
8. Security technology & integration
9. Workplace violence / active shooter prevention

Where Security Lives — Utilities & Distribution

Respondents in this sector report which function security reports to or resides within.

- CAO / Administration / Shared Services — **33%**
- CTO / Chief Technology Officer — **33%**
- Chief Health, Safety, Environment, Security & Quality Officer — **17%**
- Human Resources — **17%**

We asked The Security Benchmark Report respondents which function their security organization reports to or resides within. An even number of respondents reported to Administration and Technology. SOURCE: The Security Benchmark Report, November 2022
In the Utilities & Distribution sectors, 100% of The Security Benchmark Report respondents reported a Centralized structure of their security organization. Zero respondents within this sector reported a Decentralized or Regional structure. SOURCE: The Security Benchmark Report, November 2022

Who’s responsible for both physical security and cybersecurity?

50% of Utilities & Distribution security leaders reported being responsible for both physical security and cybersecurity.

Who’s responsible for both physical security and health & safety?

33% of Utilities & Distribution security leaders reported being responsible for both physical security and health & safety.

Geographic Security Responsibility — Utilities & Distribution
Respondents report which geographic areas they provide risk and security services to.

North America — 83%
Asia — 33%
Oceania (including Australia) — 33%
South America — 33%
Africa — 17%
Europe — 17%

The Security Benchmark Report respondents were asked to report which geographic areas their security organization provides risk and security services. Respondents were able to choose as many geographic areas as applicable. SOURCE: The Security Benchmark Report, November 2022
Within the Utilities & Distribution sector, 83% of The Security Benchmark Report respondents reported having a security operations center (SOC) or global security operations center (GSOC) within their enterprise. SOURCE: The Security Benchmark Report, November 2022

Guarding Insights — Utilities & Distribution

- **193**: Average number of enterprise-wide contract FTE security officers / guards within the Utilities & Distribution sectors.
- **67**: Average number of enterprise-wide proprietary FTE security officers / guards within Utilities & Distribution sectors.

The Security Benchmark Report respondents were asked how many contract full-time equivalent (FTE) security officers and security guards as well as how many proprietary FTE security officers / guards they have within their enterprise. The average among all respondents in the Utilities & Distribution sectors is reported here. Outliers or information that appeared to be inaccurately reported were excluded from the calculation. SOURCE: The Security Benchmark Report, November 2022
THE 2022 ACHIEVERS

TRAINING

Security Achieving Great Things in Training

The Security Benchmark Report respondents are asked to report on their initiatives, their accomplishments and their biggest focuses within their security functions. Each year, we choose a number of security leaders and teams to showcase their hard work, innovation or dedication within different categories.

The following security programs are recognized for their focus on training. Security-related training is imperative for day-to-day security operations, as well as continuity and resiliency of the organization. Training is often deployed across a number of different populations within the organization that would benefit from the subject matter. Strategic implementation of training can extend security’s reach and shine a light on the function’s value within the organization.

In 2021, Baker Hughes’ security team set a goal of targeting 40% (or 22,000 people) of its global headcount population (55,000 people) to attend security training and awareness sessions, which was a 70% increase compared to 13,000 attendees in 2020. Ultimately, 25,000 employees attended security awareness training sessions hosted by the security team in 2021, exceeding the annual goal set.
— Andrew Tosh, Baker Hughes

El Centro Regional Medical Center successfully trained 100% of its officers in de-escalation and response techniques, and the organization plans to increase training in physical response to violence.
— Bill DuBois, El Centro Regional Medical Center

GuideWell strives to be at the forefront of life safety and emergency response. The security team regularly researches the market for new developments and technologies that could enhance safety and security measures. The organization implemented the LifeVac system to supplement AED, First Aid/CPR, and Stop the Bleed programs and deployed appropriate usage training across the enterprise.
— George Frandsen, GuideWell

Materion Corporation’s security team successfully trained 2,800 U.S.-based employees on workplace violence, including practical demonstrations and drills during COVID-19. The organization also implemented a crisis management program.
— Monica N. Melas, Materion Corporation

News Corp’s security team completed best practices standards this year and implemented both enterprise-wide training and security awareness programs.
— Eduardo Jany, News Corp

The Uline Shipping Supplies’ security team has implemented a strong workplace behavioral threat assessment process and focused on training employees to be aware of potential security risks and report any concerns.
— Allen J. Innis, Uline Shipping Supplies

SOURCE: The Security Benchmark Report, November 2022

Editor’s Note: If a security program chose to remain anonymous for The Security Benchmark Report, then they were not considered for the achievements section.
The Security Benchmark Report respondents are asked to report on their initiatives, their accomplishments and their biggest focuses within their security functions. Each year, we choose a number of security leaders and teams to showcase their hard work, innovation or dedication within different categories.

The following security programs are recognized for making strides in diversity, equity and inclusion (DEI). DEI efforts can yield a stronger, more resilient security function by preparing the team for the future and bringing in diversity of ideas and thought. Ultimately, an inclusive team will aid the organization in its agility within a continually shifting threat landscape.

**Adtalem Global Education** is proud of its commitment to diversity with a breakdown of 36% female, 64% male and 37% people of color employees globally. The security team launched its Zero Harm program and continues to focus on active shooter and security awareness programs, to name a few.

— Robert Soderberg, Adtalem Global Education

**Meta’s** security team focuses on diversity, equity and inclusion (DEI) through Find, Develop and Keep pillars that enabled Global Security to represent the communities it safeguards to include under-represented communities, women, LGBTQ people, disabled people and veterans.

— Nick Lovrien, Meta

**University of Pennsylvania**’s security team expanded its transparency and inclusion efforts and continues to foster strong connections with the community it serves. As part of this effort, the organization advanced a new position of Captain of Diversity, Equity and Inclusion.

— Kathleen Shields Anderson, University of Pennsylvania

SOURCE: The Security Benchmark Report, November 2022
The Security Benchmark Report respondents are asked to report on their initiatives, their accomplishments and their biggest focuses within their security functions. Each year, we choose a number of security leaders and teams to showcase their hard work, innovation or dedication within different categories.

The following security programs are recognized for adding value and enabling the greater organization. When security treats itself as a business, the organization can drive value to its function, gain more seats at the table and, most importantly, enable — rather than prohibit — the overall organization to grow, expand and succeed.

This year, as part of its mission to constantly evolve with security risks, **AB InBev** elevated its executive protection services, along with related awareness to the program.

> — Tom Yarbrough, AB InBev

**AVANGRID**’s security team has built a world-class intelligence program that includes data feeds from the state fusion centers, Department of Homeland Security (DHS), the Federal Bureau of Intelligence (FBI) and regulators. Additionally, the program continues to invest in its insider threat program, which has recouped over $1.4 million dollars back into the organization from the cryptocurrency markets.

> — Brian Harrell, AVANGRID

Last year, **Builders FirstSource** successfully navigated a merger between BMC and Builders FirstSource, merging and integrating the Loss Prevention department into the company’s culture.

> — Randy Johnson, Builders FirstSource

**Fidelity Investments**’ Global Security and Investigations team relocated its GSOC in December 2021, which includes new operational enhancements. In 2022, there was a planned expansion to the GSOC’s role beyond traditional alarm monitoring responsibility. Enhancement efforts include increased focus on monitoring open-source and subscription-based resources for events having a potential impact on Fidelity associates and business operations, strengthening the GSOC’s intake of workplace safety concerns, and assuming an increased crisis management role in Global Security’s response to safety and security incidents.

> — Craig Magaw, Fidelity Investments

**United Therapeutics Corporation**’s security team helped support and enable the exciting science behind the first xenotransplantation of a pig heart into a human being.

> — Michael W. Wanik, United Therapeutics Corporation

This past year presented all kinds of challenges for **University Health Network**; UHN was the first Canadian hospital selected to securely house, administer and coordinate COVID-19 vaccinations. This was unchartered territory for the security team, which quickly became familiar with provincial law enforcement and prepared operating procedures to support limited distribution of the vaccine, from the airport into courier vehicles escorted by police to UHN’s secured, environmentally controlled storage.

> — Todd Milne, University Health Network

*SOURCE: The Security Benchmark Report, November 2022*
The Security Benchmark Report respondents are asked to report on their initiatives, their accomplishments and their biggest focuses within their security functions. Each year, we choose a number of security leaders and teams to showcase their hard work, innovation or dedication within different categories.

The following security programs are recognized for leading the way with new initiatives. New ideas and innovative implementations can help the security function mitigate risks and improve operational efficiency, while also streamlining business continuity and enabling informed decision-making.

**Churchill Downs Racetrack**'s security team recently modernized security protocols, which led to site-wide employee ID implementation. In addition, the Home of the Kentucky Derby is focused on growth, currently building a new 300,000-square-foot grandstand with an additional 5,500 seats, a new paddock project that will add two new clubs, several dining terraces, and double the size of the paddock area for equine athletes — and security is focused on enabling that expansion.

— Josh Ball, Churchill Downs Racetrack

**Franciscan Health**'s security team updated its patrol model to include additional physical and electronic security and enhancements that include updates to video and access control systems. The technological enhancements have reduced officer response times to incidents and helped reduce cases of workplace violence with injuries. The organization has also seen a reduction in attempted elopement from high-risk areas of the campus. In addition, the security team implemented a contraband screening program to help reduce the likelihood of illegal contraband (narcotics and/or weapons) within their facilities.

— Daniel Lempa, Franciscan Health Olympia Fields

**The Jackson Laboratory** in Bar Harbor, Maine, implemented a robust international travel security program this past year. In addition, for the rest of this year and into 2023, the organization’s security team will focus on enabling a more tech-savvy workforce beyond the traditional sets of skills required.

— Brian O’Rourke, The Jackson Laboratory

**Geisinger** completed a security department leadership reorganization, which created a systemwide department including an associate vice president, two regional directors, and a systemwide director of training and special programs. In addition, the organization is working toward transitioning to sworn law enforcement staffing and has established a tiered system of workplace violence committees. Security services is actively promoting the reporting of workplace violence incidents and, within the coming year, each hospital campus is expected to implement mobile duress alarms for site employees.

— Sean McGinley, Geisinger

**Global Atlantic Financial Group** developed security metrics for the first time to prove value, focus on efficiency and improve operations.

— Robert Shickel, Global Atlantic Financial Group

**Sparrow Hospital** implemented a canine program with a primary focus on narcotics. The program also detects munitions and serves as a de facto therapy program for the organization, as dogs are trained to allow for contact with the public. The canine program has increased accuracy of room searches for patients suspected of narcotics usage.

— Jerry Dumond, Sparrow Hospital

One of **Wellstar Health System**'s security department’s achievements over the past year and a half has been increasing security staff by 59%. In addition, the organization added enhanced workplace violence training and policies; increased access control, cameras and duress alarms by 35%; added metal detection devices in all 11 hospitals; and enhanced facility security design, including lighting, physical barriers, etc.

— Adrian Arriaga, Wellstar Health System

**Whirlpool Corporation**’s security team implemented its first-ever enterprise-wide crisis management program and plans to focus on its first-ever security audit program this year and into 2023.

— Erik Antons, Whirlpool Corporation

**SOURCE:** The Security Benchmark Report, November 2022

---

Editor’s Note: If a security program chose to remain anonymous for The Security Benchmark Report, then they were not considered for the achievements section.
The Security Benchmark Report respondents are asked to report on their initiatives, their accomplishments and their biggest focuses within their security functions. Each year, we choose a number of security leaders and teams to showcase their hard work, innovation or dedication within different categories.

The following security programs are recognized for their focus on retention and development. Many security teams have experienced the same hiring and retention challenges of organizations around the world. But security never sleeps and security functions have had to get creative, thoughtful and deliberate to ensure operational continuity and positive work environments.

AdventHealth Central Florida Division’s security team has seen significant increases in its quality of hire, overall employee satisfaction, and willingness for employees to recommend the organization as a place to work. Also, the organization had two security directors voted as finalists for the OSPA awards.
— Christopher C. Fender, AdventHealth Central Florida Division

Ballad Health’s security team worked with Human Resources to request a wage market adjustment for security officers. The wage adjustment helped with officer retention. In addition, the organization armed all officers in the health system and expanded security officer force-on-force Simunition training, giving officers “shoot, don’t shoot” scenarios that could — or have — happened in a healthcare setting.
— Ken Harr, Ballad Health

GE Healthcare’s security team has focused on the mental wellbeing of employees throughout the COVID-19 pandemic, prioritizing mandatory work breaks for remote workers and exploring and implementing proactive gamification training for cybersecurity.
— Shiva Rajagopalan, GE Healthcare

SOURCE: The Security Benchmark Report, November 2022

Editor’s Note: If a security program chose to remain anonymous for The Security Benchmark Report, then they were not considered for the achievements section.
THE 2022 ACHIEVERS

TECHNOLOGY

Security Strategically Using Technology

The Security Benchmark Report respondents are asked to report on their initiatives, their accomplishments and their biggest focuses within their security functions. Each year, we choose a number of security leaders and teams to showcase their hard work, innovation or dedication within different categories.

The following security programs are recognized for their security technology implementations. Technology, solutions and systems can be extremely beneficial for security functions in improving efficiencies, security operations and eliminating or easing pain points, such as workforce challenges or human error.

In 2022, Baycrest Centre for Geriatric Care opened a new, purpose-built security operations center for the first time to emphasize and focus on security. The organization is also adding an RTLS System for wireless mobile staff duress, asset tracking and at-risk patient monitoring.
— Martin Green, Baycrest Centre for Geriatric Care

This past year, Denver Health Medical Center added an OSINT platform to better monitor and track risks as well as persons of interest and threat assessments to manage responses to violent behavior.
— Eric Smith, Denver Health Medical Center

For 2022 and into 2023, Gap Inc. is focusing on fewer apprehensions to create a safer environment, as well as building stronger relationships and partnerships with law enforcement and other asset protection organizations. Currently, the organization is piloting radio frequency identification (RFID) and Bluetooth low energy (BLE) solutions.
— Chris Nelson, Gap Inc.

This year, GoDaddy developed processes and deployed technology surrounding critical event management to ensure business resiliency and operations continuity.
— Jason Veiock, GoDaddy

Kimberly-Clark has made a significant transformation to operations by using security technology to automate routine security procedures, resulting in savings on security guard spend.
— John A. Johnson, Kimberly-Clark

One of the way’s Orlando City Soccer Club’s security team is enhancing its presence is through an app that puts vital safety and security information in the hands of every employee. The team developed multiple digital pages and each page links to QR codes, which are dedicated to each segment of the organization, including vendors, employees and each training facility. In addition to digital technology, the security team is focused on perimeter security, including adding bollards for vehicle mitigation and coordinating plans to fence and gate the external perimeter — ultimately pushing security screening further away from the venue.
— Robert Schnettler, Orlando City Soccer Club / Exploria Stadium

SOURCE: The Security Benchmark Report, November 2022

Editor’s Note: If a security program chose to remain anonymous for The Security Benchmark Report, then they were not considered for the achievements section.
More About The 2022 Security Benchmark Report — Methodology

The purpose of The Security Benchmark Report is to create a database to measure security teams and organizations versus their peers, both among the industry as a whole and among individual sectors, for even better comparison. Security magazine’s number one goal with The Security Benchmark Report is to showcase the value of security within the enterprise, as well as be a business enabler to our readers’ security programs.

Organizations are able to remain anonymous for this survey. If the organization chooses to be marked anonymous, they are not eligible to be listed in the published report’s metrics listings or achievement sections.

All information within this report is based on The Security Benchmark Report survey responses. Organizations may only fill out the survey once for a particular company or agency. Security programs within the rankings must be responsible, at least in part, for physical security within the enterprise. The Security Benchmark Report does not include contract security companies, guarding companies or those without a level of direct responsibility for security within their enterprise.

The Security Benchmark Report is broken down into a general overview comparing all respondents’ data with one another, as well as by sector. Respondents are asked which sector their overall enterprise resides in and this is the sector in which they are placed. While the survey has a choice of 22 market sectors, some sectors are chosen by too few respondents to report on individually. Therefore, for better comparisons, some market sectors are combined in the report. Combined sectors are labeled as such, and combinations may vary each year.

Sectors with too small a dataset that don’t lend themselves to combining with other sectors may be excluded from the sector reports, but will be included in the main report. To attempt to make the most meaningful comparisons, particular comparisons/charts are left out of sector groupings if the data varied too greatly from one respondent to the next.

In some cases, when calculating certain statistics, including “security budget as a percent of revenue,” outliers are removed before calculations to present a cleaner comparison.

While we recognize that security roles, responsibilities and programs can vary widely from one organization to another in terms of maturity, position within the enterprise, size of staff, budget, etc., Security has made every effort — due to input from readers and Editorial Advisory Board members — to break down and compare organizations in a meaningful, valuable way.

If you don’t see your enterprise’s primary market sector represented, we encourage you to fill out the survey and ask your peers to fill out the survey as well. The more organizations and security professionals that fill out the survey, the more robust the data. Each year, the survey opens in February and closes in July.

Security magazine encourages all security leaders and organizations to participate in this free editorial survey that makes up The Security Benchmark Report. As a benefit to filling out The Security Benchmark Report survey, security leader respondents receive a full (anonymized) report of responses with more detailed information beyond what is covered in Security’s November eMagazine and online.

The Security Benchmark Report is an editorial project, and respondent contact information collected is not sold or shared.

www.SecurityMagazine.com