tyco
Security Products

Cybersecurity Vulnerability Management:

Finding Your Enterprise’s Security Product Partner

William L Brown Jr.

Senior Engineering Manager, Regulatory and Product Security

Is your security system doing its part to protect your enterprise from data breaches?

With more and more security technology running on the network, installing security devices without cybersecurity is the equivalent of leaving service doors unlocked for your office building. Just because the main doors have access control does not mean the figurative attacker cannot enter the building through those few unlocked side doors. The same is true for your network.

Take, for instance, the Turkish oil pipeline that mysteriously caught fire in 2008 without triggering alarms or sensors. Investigators found that malicious hackers had used a vulnerable security camera to gain access to the pipeline's control network. Once inside, they found a vulnerable PC to install a backdoor that allowed them to access the network whenever they wanted. They were able to take their time and explored the system before finally increasing the pressure in the pipeline – all without alerting the control room. Besides the environmental impact, the attack cost BP, the State Oil Fund of the Republic of Azerbaijan, and others millions of dollars.

Although cyber attacks resulting in physical damage are extremely rare, as seen in recent headlines, attacks that result in the theft of customer or patient data are becoming more prevalent and garnering more attention in the press. Not as well reported, but much more common, is the deletion or ransom of data. The FBI released a warning in December 2014 about a destructive malware campaign that can overwrite data files in a way that makes it "extremely difficult and costly, if not impossible, to recover the data using standard forensic methods." Doctors' offices and even police stations have been forced to pay ransom to their attackers to recover their own data after it was made inaccessible to them. This could put an enterprise in recovery mode for weeks, months, or worse. For example, in 2012, a global energy company based out of the Middle East lost use of its internal network services after a virus rendered 30,000 of its computers inoperable. Even though the company had an effective backup and recovery strategy in place, rebuilding the internal network took 10 days.

IT professionals for enterprise-level organizations are already placing their requirements on devices before allowing them to connect to their network, but even small and medium sized networks should consider the potential impact if their data is stolen, deleted, or held for ransom. With such a high potential impact to an organization, cybersecurity cannot be an afterthought, even for physical security products. Security integrators need to know the impact to their business if their installed system was the reason for a major breach.

How Do Security Devices Impact Cybersecurity?

Security devices, such as IP surveillance cameras or access control devices, are not often the target of cyber attacks, but merely the entry point for hackers to get a foot in the door of your network. As in the case with the pipeline, when an attacker finds a vulnerable device such as a camera, they can use it to find a path back to the larger enterprise network and find a vulnerable device to infect. There they can exploit the device by installing ransomware, stealing data, or performing any number of malicious activities.

The most difficult part of cybersecurity is that hardening devices alone will not safeguard your network. Any device that was secure today can be vulnerable tomorrow, as was seen in 2014 with the announcement of ShellShock or Bash Bug. This critical bug in GNU Bash gives an attacker multiple ways to execute arbitrary code on a device, most of which do not require authentication. It is so easy to detect a vulnerable device that within hours of ShellShock's announcement, hackers were searching for prey. At one point, the rate was up to almost 2,000 attacks per hour. GNU Bash is so prevalent in Web and email servers (and even security devices) that the announcement immediately made millions of devices vulnerable, except, in truth, the vulnerability had existed undetected by the public for 25 years.

This is the nature of cybersecurity. You must assume you are vulnerable at all times, and you must be prepared to do whatever you can to address each vulnerability as it arises.

With ShellShock, IT professionals, while scrambling to minimize the damage to their network, began to issue their ultimatum: “Fix your device, or it’s off our network!” Consider the potential impact of this on your security system. This could mean your control panels, NVRs and more could be banished from the network, leaving your security system crippled.

Security leaders cannot afford to wait until they receive that ultimatum to consider cybersecurity for networked systems. They must have answers for IT professionals as to how security systems are protected, and getting those answers starts with asking your vendors the right questions.

What Should I Ask My Vendors?

1) Do you have a cybersecurity program?

   Do not accept a “yes” or “no” answer here. Details are necessary to help you defend your program to the IT department and the C-Suite, and to help you evaluate and compare new vendors.

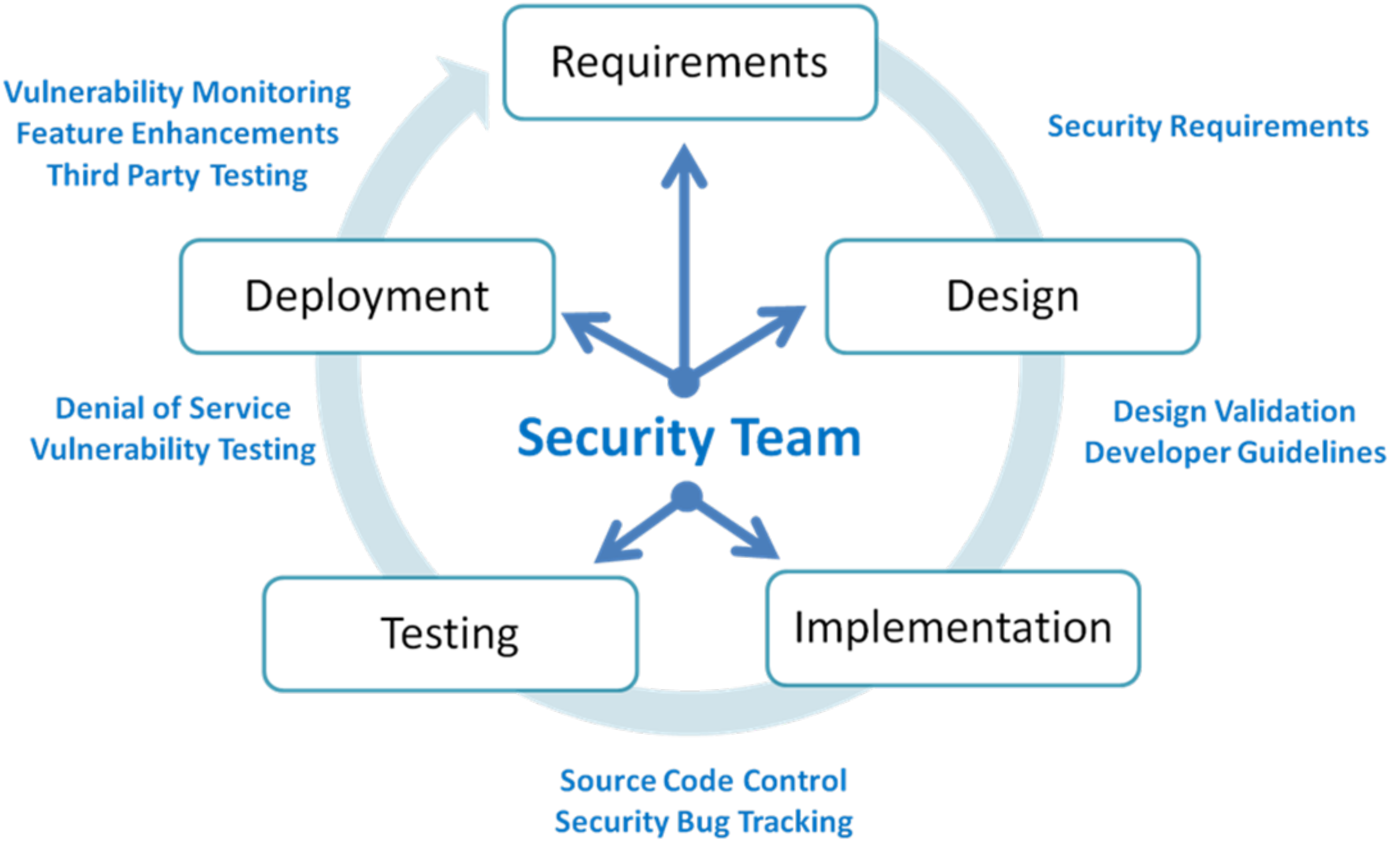
   Did you catch the vendor off guard? If the vendor truly has an established cybersecurity program, they should be prepared to discuss their initiatives.

   Do they have a dedicated cybersecurity staff, or are they relying on their engineers? There are pros and cons to each. A dedicated team might not be as familiar with the products, but product engineers already have full-time jobs and may not be able to respond as quickly. A cross-functional team often serves best in this regard, with dedicated development engineers who can be pulled from their current assignments to respond quickly to new vulnerabilities.

   How long has the program been active? Consider your risk appetite for working with a fledgling cybersecurity program. Ask for published whitepapers or other resources to help determine the quality of the program. Ask for the supplier’s cybersecurity mission and product statements, as well.

2) How is cybersecurity part of the product development process?

Is cybersecurity an integral part of the device's development process, or is it an afterthought added to the nearly-finished product? Every product has a development cycle, and it starts with the requirements. Security should be part of the consideration when the concept of a new product or feature is first proposed. Then, as the process moves from concept to design and into implementation, secure design methodologies should be used. Security should be tested before deployment to ensure vulnerable devices are not released. Finally, after deployment, efforts must be taken to monitor and respond to new vulnerabilities and feedback enhancements to the next revision of the product.



3) How do you alert users to new vulnerabilities?

While security executives should have their own vulnerability alerts in place (good examples include alerts from NIST’s National Vulnerability Database, the U.S. Computer Emergency Readiness Team, or other media and professional outlets), suppliers should keep their users informed about any remediation for those vulnerabilities.

When evaluating your supplier’s cybersecurity response capabilities, ask to see examples of what they have done in the past. Make sure that they are actually providing resolution and not just alerting you that you are vulnerable. Also, consider how vulnerabilities are assessed prior to an alert. Who is performing the assessment? How quickly are advisories provided? What is the average turnaround time for patches?

4) How do we best partner together on cybersecurity?

Just as enterprise security leaders want a long-term partner as their security system integrator, you also want a good cybersecurity partnership with your supplier. Find out how you can inquire about vulnerabilities or best hardening practices. A good supplier partner will want to help you succeed beyond the product sale. Ask to discuss the supplier’s product roadmap as it relates to cybersecurity. Determine who the best points of contact for cybersecurity topics are within that organization. Having access to a good cybersecurity team can be your biggest asset for meeting evolving needs.

When working with government data or networks, or securing critical infrastructure sites, you will be required to meet certain regulatory requirements. The U.S. Federal Information Security Modernization Act (FISMA, formerly the Federal Information Security Management Act), originally passed in 2002 and updated in 2014, requires each federal agency to develop, document and implement an agency-wide information security program for in-house and thirdparty information systems, including those provided or managed by outside agencies, contractors or other sources.

5) What is your experience with the NIST Risk Management Framework?

To comply with FISMA, most agencies have adopted the Risk Management Framework (RMF) developed by the National Institute of Science and Technology (NIST) which provides a method to access a system and apply and monitor security controls on the products, installation and operations processes. Historically, the Department of Defense had used DIACAP for compliance with FISMA, but that has recently been replaced by DIARMF, which is based on the NIST RMF.

An organization with knowledge and experience with the NIST RMF will help ensure the products can be configured to help an installation comply with the certification and authorization process required by FISMA.

While FISMA applies specifically to any organization that stores or transmits government-owned data, for private sector enterprises, the NIST RMF provides sound guidance to build a cybersecurity program and help demonstrate an enterprise's due diligence in working to protect data.

Conclusion

Are you prepared to answer the tough questions on cybersecurity from an end user or IT professional? Does your product vendor have a security program, or is security an afterthought? Can the vendor quickly correct for new vulnerabilities? If you are not sure, then it is time to assess your cybersecurity readiness. After all, what if the headlines of the next breach are caused by a security system you rely on or installed?

For more information about Tyco Security Products' approach to cybersecurity, contact William Brown at willbrown@tycoint.com