# USING TECHNOLOGY WISELY TO PROTECT YOUR ORGANIZATION

by Greg Porter

## WHEN SEARCHING FOR INFORMATION SECURITY TECHNOLOGIES TO PROTECT YOUR ORGANIZATION FROM CYBER-RELATED THREATS,

being an informed consumer can help to ensure that you invest in the right solutions for your business. One way to accomplish this is to align investment decisions with the overall risk management processes of the organization.

### RISK MANAGEMENT

Addressing vulnerabilities is often perceived as taking a risk-based approach to information security management; however, it's essential that the business focus on the right areas. Accounting for cyber-related risks should be focused on quality, not merely the quantity of vulnerabilities and threats mitigated. Taking a risk-managed approach means the organization has identified relevant threats to the business, acknowledging the realities of limited staffing, budgeting and the fact that not every observed risk can and should be addressed. Prioritization means the organization directs its resources towards high risk issues, specifically those with a high degree of likelihood and impact, as opposed to fixing vulnerabilities that aren't linked to meaningful threats that can disrupt the business and its mission. Enterprise risk management processes provide decision support via annual assessments such as internal/external penetration testing, vulnerability assessments, compliance audits and network security monitoring observations, all in an effort to identify weaknesses and gauge potential damage to the business. Investment decisions can then be made to acquire technologies that clearly address high-priority risks based on their likelihood of occurrence, the costs associated should the risk occur, and the estimated cost to correct it.

> "Accounting for cyber-related risks should be focused on quality, not merely the quantity of vulnerabilities and threats mitigated."

Risk management processes can also be used as an enterprise surveillance mechanism to proactively identify technologies—cloud-based services, the Internet of Things ("IoT"), mobile device management—that the oganization may be considering using. Instead of viewing the usage of such technologies as a binary decision, take measures to decide whether (and how) they can be implemented successfully and securely by conducting an assessment of potential risks and exposures to the business. The process can help the business make an informed decision as to whether it's fully ready, partially ready or not at all ready to integrate the proposed software or hardware into its production environment. Based on these findings, administrative, physical and/or technical safeguards can be evaluated to manage risk to an acceptable level.

## PRACTICAL VENDOR MANAGEMENT

Being an informed consumer when working with vendors will help. Once you've identified information security technologies that align with your risk management activities and business process needs, identify vendors that provide that technology and rely on your technical personnel to keep you informed of the technology options that are available. Remain mindful of acquisition costs and the total cost of ownership—there's the price that the vendor provides for the hardware/software, but what costs will be associated with installing, configuring, tuning, training, monitoring and maintaining the solution over time? Ensuring this is accounted for can remove unexpected surprises in the budget.

"Most vendors will let you deploy their product on a test network so that your staff can evaluate how well it may work in your environment..."

Lastly, work with your vendors to establish a proof of technology. Most vendors will let you deploy their product on a test network so that your staff can evaluate how well it may work in your environment as well as how it compares to peer products. This approach is a powerful way to evaluate solutions with minimal capital investment and can help the business separate fact from fiction in the marketplace.

## TRAINING

As the past several years have demonstrated, adversaries often operate within a network for several months before they are detected. Rapid, systematic detection of cyber intrusions is a business imperative and so too is having capable talent to assist. Good protection is less about the technologies involved and more about the people interacting with them to help the business make wise, risk-based decisions. Today's threat landscape is one of constant evolution; because of this, adequately invest in training your staff to maintain and improve upon preparedness. Take measures to help them expand upon their existing skill sets and knowledge through internal and external training programs. Information security is a dynamic field. Identify what areas they are most interested in and collaboratively assist them with developing a performance measurement plan that will not only help them improve upon existing skills, but also help to further secure the business by making sure they are well informed about current and emerging threats and how to monitor and address them.

"Taking a risk-managed approach means the organization has identified relevant threats to the business..."

## GETTING HELP

Using these strategies will help you to navigate a dynamic environment of changing technology and risks in a way that enables you to focus on the safeguards that will benefit your organization the most. Technology must be viewed, evaluated and used through the lenses of risk management, cost-benefit analysis, and highly skilled and trained people.

**Greg Porter** is the Founder of Allegheny Digital, an information security consultancy specializing in enterprise risk management, incident response, and managed threat monitoring. Mr. Porter graduated from the University of Pittsburgh, received his master's degrees from Carnegie Mellon University, and holds a number of professional certifications. He also serves as a Cybersecurity Researcher for the SEI CERT.

"Addressing vulnerabilities is often perceived as taking a risk-based approach to information security management; however, it's essential that the business focus on the right areas."