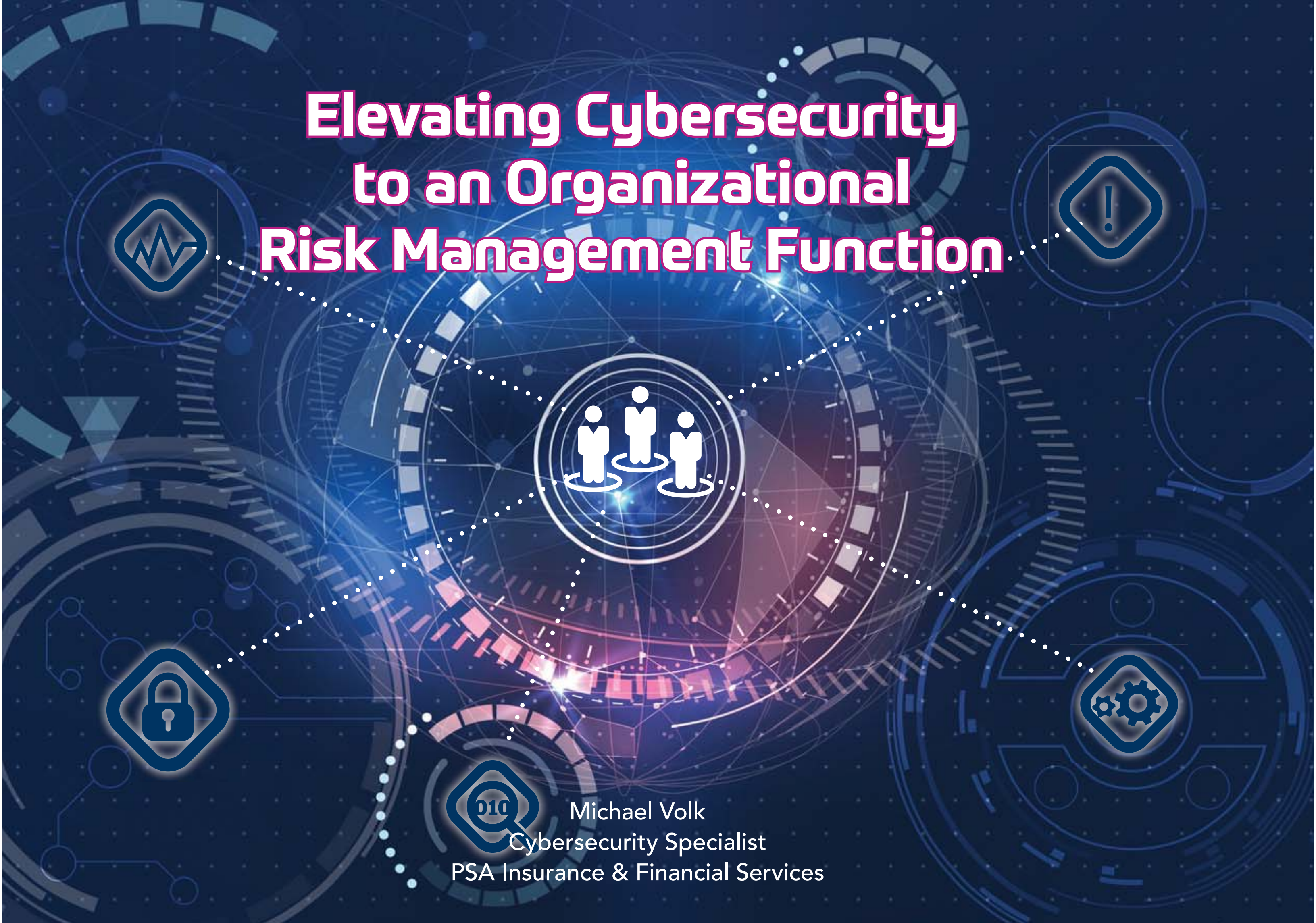


Elevating Cybersecurity to an Organizational Risk Management Function

Michael Volk
Cybersecurity Specialist
PSA Insurance & Financial Services

The environment of cybersecurity is complex and uncertain, but it is at times framed in the context of a game that is predictable and defined by rules. This approach can lead to an overreliance on advanced cybersecurity tools to predict and prevent incidents. It may also result in placing too much pressure on IT experts to succeed 100% of the time in an asymmetric environment where cybercriminals dictate the terms and only have to succeed once to cripple an organization.

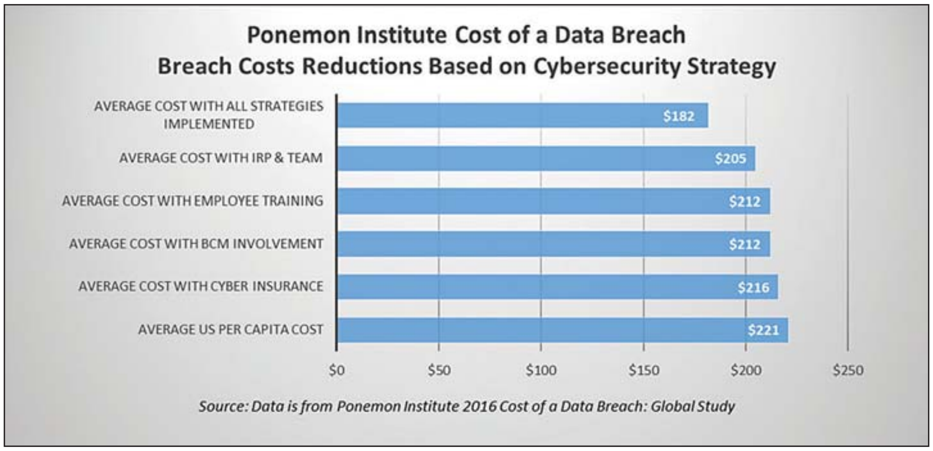
It is helpful to use tools and models based on available empirical data to guide our actions in times of great uncertainty. This is a good strategy and has led to incredible advancements in cybersecurity. The challenge, however, arises when the cybersecurity strategy of an organization is based solely on technology, which makes the organization blind to threats that are not anticipated. Add the human element – the epitome of unpredictability – to the equation, and succeeding in cybersecurity when it is framed as a zero sum game quickly becomes unrealistic. In order to reduce risk and the impact of a cyber breach, we must begin to shift cybersecurity from an IT task to a risk management function that involves the entire organization, including leadership.

Framing cybersecurity as a game is a good example of the Ludic Fallacy that Nassim Nicholas Taleb describes in his book The Black Swan. According to Taleb, the Ludic Fallacy grows out of a sterilized and domesticated view of uncertainty, similar to what you might find in a casino. In the case of such an establishment, "you know the rules, you can calculate the odds, and the type of uncertainty we encounter there is mild. You cannot expect a casino to pay out a million times your bet, or change the rules abruptly on you during the game."[1] Unlike games of chance played in a casino, however, uncertainty in cybersecurity is extreme, the rules are constantly changing, and prediction is only partially effective because our data-driven models cannot account for threats and vulnerabilities that have not yet been observed. To effectively respond and recover from a

Taking the initial steps to integrate cybersecurity and BCM can be challenging, but the investment in time can lead to both long-term and immediate benefits.

cyber-attack, organizations must avoid falling for the Ludic Fallacy in cybersecurity.

Elevating cybersecurity from an IT function to a holistic, organization-wide approach is a good way to avoid falling for the Ludic Fallacy. This idea is not a revolutionary concept and is becoming quite common in the industry, as cybersecurity and business professionals alike see the value in viewing cybersecurity as an organizational risk management issue rather than a purely IT function. Yet, making this shift can be overwhelming and difficult for a variety of reasons. While far from comprehensive, here are a few areas of focus that organizations can explore in the process of elevating cybersecurity to an organizational risk management function.



Source: Data is from Ponemon Institute 2016 Cost of a Data Breach: Global Study

Integrate Business Continuity Management and Cybersecurity

Business continuity management (BCM) is a process designed to help identify risks, threats, and vulnerabilities that can lead to business interruption and serious negative financial implications. Developing safeguards that help reduce risk, as well as processes for responding when something does go wrong, are also part of the BCM process. Many organizations already have a BCM process in place related to their operations, but they manage their cyber risk as a separate task. A good first step towards elevating cybersecurity to an organizational issue is to integrate BCM and cybersecurity risk management.

One effective way to start the integration process is to use existing cybersecurity risk frameworks that align with the BCM process to guide the integration of the two. There are several cybersecurity risk framework options to choose from, but a great place to start is with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The NIST Cybersecurity Framework includes five core functions (Identify, Protect, Detect, Respond, and Recover) that are designed to help form "an operational culture that addresses the dynamic cybersecurity risk."[2] The NIST publication also includes additional guidance, including informative references to assist with implementation.

Taking the initial steps to integrate cybersecurity and BCM can be challenging, but the investment can, in time, lead to both long-term and immediate benefits. Long-term benefits will be realized as the organization becomes better equipped to defend, respond, and recover from cybersecurity breaches and incidents. Short term benefits can be seen in the reduction of the cost of a breach, should one occur. According to the Cost of a Data Breach study published by the Ponemon Institute in 2016, organizations with BCM involvement can reduce the cost of a data breach by $9 per record.[3]

Create an Incident Response Plan and Practice

Another effective strategy to integrate cybersecurity into the organizational risk management process is to develop an incident response plan (IRP) and team to carry it out. Creating an IRP not only provides a documented plan that can guide actions in the event of a cybersecurity incident, but also helps build a cross-functional team of internal and external stakeholders who are involved in the response process. The necessary activity of creating an IRP will also help stakeholders and leadership see firsthand that the IT and management functions of cybersecurity are directly connected. For example, an

In order to improve cybersecurity and help foster a culture of awareness, training should be an ongoing investment for both the technical and non-technical workforce.

IRP's communication process includes members of IT, management, and leadership, as well as legal counsel and insurance professionals.

Another important step in creating an IRP is practicing. Conducting tabletop exercises is necessary to make sure stakeholders know what to do, and to ensure that implementation issues are worked out prior to a live event. Practicing an IRP ensures that the strategy can be executed in real time, but also carries the added benefit of further exemplifying the connections between IT and management functions as they relate to cybersecurity risk management. In addition, creating an IRP and team to carry it out can reduce the cost of a breach by as much as $16 per record, according to the 2016 Ponemon institute study.[4]

Training

Organizations often fail to dedicate the necessary resources to training. In order to improve cybersecurity and help foster a culture of awareness, training should be an ongoing investment for both the technical and non-technical workforce.

IT staff should be up to date on current threats, defense strategies, and technologies. According to the Intel Security and the Center for Strategic and International Studies, "more than two-thirds of information technology executives said low IT security staff sizes made organizations at risk for direct and measurable damage and desirable hacking targets."[5] Because of this need, cybersecurity professionals are in demand, but the supply of talented professionals is limited. Offering a training plan that aligns with your cybersecurity needs will not only bolster the defense of your organization, but can potentially allow your organization to develop and grow its own workforce instead of competing for top professionals in the open market.

Training is important for non-technical staff as well. Meaningful cybersecurity awareness training contextualized for your workforce using real examples of threats, technology use policies, cybersecurity technology, and what to do when something goes wrong can go a long way in improving cybersecurity. Cyber-aware technology users can have the effect of embedding human sensors in the network that will become great assets to the IT and cybersecurity team. As shown in the other examples presented here, training can also reduce the cost of a breach by $9 per record.[6]

Cybersecurity Insurance

The financial implications of a breach can devastate an organization. According to the Ponemon study, the average cost per piece of lost or stolen data is $221 for an organization in the US.[7] The definition of what constitutes a data breach will vary, but a representative sample of the type of information that must be protected includes: driver's license numbers, first and last names, Social Security numbers, home addresses, tax ID numbers, credit and debit card information, CVV numbers, phone numbers, diagnosis codes, dates of birth, travel information, diagnostic information, e-mail addresses, bank information, healthcare records and insurance numbers, employee payroll information, passport numbers and contact information, salary information, and employee ID numbers, as well as mobile banking usernames and passwords. In addition to the extensive and growing list of information that must be protected, there are 47 different state data breach notification statutes that organizations may be required to comply with after a data breach. Responding to a data breach can include legal fees, individual notification costs, credit monitoring services, and forensics, as well as other costly components that add up quickly.

Cyber risk is very difficult to avoid, as most organizations store electronic data, communicate electronically, have a web presence, and rely on technology to conduct business. While cyber risk exposure will vary from one organization to the next, there are common risk themes. Organizations processing and storing credit card payments, managing large amounts of personally identifiable information (PII), personal health information (PHI), or confidential corporate information can face serious financial and legal implications if this information is compromised.

Others that might not handle this type of information are exposed in other ways. According to the 2015 Data Breach Investigations Report published by Verizon, a large number of website attacks include a secondary victim where "the actors have no real interest in the owner of the website other than using the owner to further the real attack."[8] Even if your organization is not the primary target of a cyber-attack, you are still at risk of becoming a victim. The financial costs, combined with the fact that cybersecurity incidents are difficult to predict or prevent, make cybersecurity insurance critical for the long term viability of all organizations.

In addition to the financial and risk transfer benefits of cybersecurity insurance, the process of purchasing this type of insurance is another effective exercise to help elevate cybersecurity to a management function. Selecting cybersecurity insurance includes a process of placing a value on the organization's digital assets, exploring threats and risks, and evaluating the cybersecurity strategies currently in place. This process can be both challenging and eye-opening for all involved, and will require input from many stakeholders across the organization.

Cyber insurance coverage available today protects against a number of exposures, some of which include liability to others, direct costs from fines and penalties, business interruption, contingent business interruption, and other expenses. Protection for these risks can have different coverage triggers, insured limits, self-insured limits, or deductibles. While there may be some commonalities in the coverages, all policies available from the more than 90 companies offering cyber insurance are different. Further complicating the process is that cybersecurity insurance needs and benefits will vary from one organization to the next. Needless to say, choosing cybersecurity insurance can be confusing.

The best strategy to start the process is to consult with a trusted insurance advisor to help find the most appropriate coverage option for your organization's unique exposures, which can reduce the cost of a data breach by $5 per record.[9]

Cybersecurity continues to be a challenge for all organizations as we become increasingly reliant on technology, and as threats and vulnerabilities continue to evolve. As we move further into the cyber age, organizations that elevate their cybersecurity strategy beyond an IT function to an organizational approach will be better positioned to manage cyber risk, and to respond if and when a breach or incident occurs.

About the Author:

Michael Volk *serves as PSA's Cybersecurity Specialist. In his previous roles, he focused on cybersecurity workforce development to help individuals and organizations navigate the complex cybersecurity landscape through training, raising awareness and by advocating for cyber organizational development strategies. Mr. Volk holds a M.P.A. from the University of Baltimore and a B.A. in Political Science from McDaniel College.*

PSA
INSURANCE & FINANCIAL SERVICES

Sources

1. Taleb, N. N. (2010). The black swan. New York: Random House.
2. National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity.
3. Ponemon Institute. (2016). 2016 cost of data breach study: Global analysis. Traverse City: Ponemon Institute LLC.
4. Ibid.
5. Wilkers, R. (2016, August 31). Noblis' Roger Mason: Career path understanding key to cyber workforce training, returning efforts. Retrieved from ExecutiveBiz: http://blog.executivebiz.com/2016/08/noblis-roger-mason-career-path-understanding-key-to-cyber-workforce-training-retention-efforts/
6. Ponemon Institute. (2016). 2016 cost of data breach study: Global analysis. Traverse City: Ponemon Institute LLC.
7. Ibid.
8. Verizon Enterprise Solutions. (2015). 2015 data breach investigations report.
9. Ponemon Institute. (2016). 2016 cost of data breach study: Global analysis. Traverse City: Ponemon Institute LLC.