INTELLIGENT RISK

knowledge for the PRMIA community

May 2017

PRMIA
The Professional Risk Managers' International Association

closing the cyber security risk door

by **Mark** Trembacki

Many current approaches to managing cyber security risk embody the idiom, “shutting the barn door after the horses are gone.” The implications of such short-sighted cyber security risk management practices are significant, with 60% of small companies estimated to be unable to sustain their business within six months of a cyber-attack,[1] and a prediction that a Fortune 1000 company will fail in 2017 as a result of a cyberbreach.[2]

This article describes three practical steps to close the cyber security risk door before it’s too late.

1. Heed the basics to avoid cyber incidents, by deploying existing tools and proven practices.
2. Build resilience as well as prevention for a swift response and successful recovery.
3. Leverage enterprise risk management practices to enhance cyber security management.

This three-fold approach is not intended to shortchange the need for a strong technological defense, which is an essential ingredient to combat the ever-increasing sophistication of threats. However, technology alone is not the answer.

heed the basics

The Commission on Enhancing National Cybersecurity, formed by executive order of President Obama in 2016, recently reported:

> ***“Many organizations and individuals still fail to do the basics. Malicious actors continue to benefit from organizations’ and individuals’ reluctance to prioritize basic cybersecurity activities . . . . . these failures to mitigate risk . . . . . allow malicious actors of any skill level to exploit some systems at will.”*** [3]

Training employees, managing vendor environments, and securing physical assets figure prominently among implementation basics to achieve strong cybersecurity practices.

1 / House Small Business Subcommittee on Health and Technology March 2013 Hearing.

2 / Forrester 2017 Predictions October 2016 Report.

3 / Commission on Enhancing National Cybersecurity December 2016 Report.

Engaging employees → The first line of defense

Wombat Security Technologies and the Aberdeen Group found that “an investment in user awareness and training effectively changes behavior and quantifiably reduces security-related risks by 45% to 70%.”[4] Employee education topics should include authentication (passwords), e-mail practices, social media, social engineering and phishing, network connections, and restricted user installation of applications.

Managing vendors and external partners

Companies manage hundreds of vendor, third-party service providers, and outsourcing arrangements. These external partners represent a primary source of incremental risk by creating entry points into a company’s technology environment. Through widespread use of vendors, data management is no longer fully in control of the organization, adding complexity and risk.

Legal and other practical considerations should be employed to partition and mitigate the risk. However, a strong third-party vendor management program is essential to manage cyber security risk. Beyond strengthening cyber security risk management, a robust program helps achieve core business objectives by supporting spending decisions, contracting strategies, service levels, and other critical operational activities.

Securing the physical world

Stolen laptops remain an issue. Bitglass, a data protection company, noted an organization is more likely to be robbed than hacked.[5] Company policies and employee training should cover physical protection of mobile devices (laptops and smartphones), USB drives and other portable storage devices, as well as device access.

Physical security should also be incorporated into policies and employee awareness building. Limiting and monitoring access (particularly to high risk areas), discouraging tailgating, securing desktop computers, and implementing clean-desk practices enhance data security.

building resilience and prevention

The detection and prevention of a cyber attack remains a critical and ever-present activity. However, resiliency – the ability to anticipate, prepare for, and recover from – a cyber attack should also be a point of focus. Many believe a cyber incident is a matter of “when” not “if”. Planning for a wide variety of threats and outcomes will support faster recovery from cyber incidents.

4 / Wombat Security Technologies and the Aberdeen Group January 2015 Report.

5 / Bitglass 2014 Healthcare Breach Report.

Compared to other risks, cyber risk can be instantaneous, impact a large number of users, be highly visible and difficult to remediate. Social media and instant news feeds accelerate the spread of the news, increasing the need for quicker response times. Establishing relationships with external experts and firms can also support a more decisive response to a data breach.

leveraging enterprise risk management practices

The use of digital technology, and therefore the vulnerability to cyber disruption, is present in most business activities. Utilizing existing practices to assess, manage, and oversee cyber security risk will be more effective than implementing standalone processes solely designed to cover cyber security risk.

Organizational processes that should be reviewed for cyber awareness include: strategic planning, M&A, product development, capital allocation and budgeting, vendor management, business continuity planning, and talent management. Incorporating a “cyber filter” into organizational processes enhances cultural awareness as well as facilitates a cross-functional, enterprise-wide approach to yield a holistic, “birds-eye” view of this highly complex risk.

conclusion

Creating value means taking risk. The classic risk and return paradigm applies to cyber security risk, notwithstanding its unique characteristics and pervasive nature. Cyber security risk can’t be avoided, but it can be managed. Developing a cost-effective strategy based on a consistent and comprehensive information security framework will go a long way to support a company’s security, resilience, and overall cyber security confidence.

references

1. Bitglass. 2014 Healthcare Breach Report. “Healthcare Breach Report.”
2. Commission on Enhancing National Cybersecurity. December 2016 Report. “Report on Securing and Growing the Digital Economy.”
3. Forrester 2017 Predictions. October 2016 Report. “2017 Predictions.” Forrester.com. October.
4. House Small Business Subcommittee on Health and Technology. March 2013 Hearing. “Protecting Small Businesses Against Emerging and Complex Cyber-Attacks.” Hearing Findings, Washington, D.C.
5. Wombat Security Technologies and the Aberdeen Group. January 2015 Report. “The Last Mile in IT Security: Changing User Behavior.”

author

Mark Trembacki

Mark Trembacki teaches Enterprise Risk Management in the Masters of Finance program at the University of Illinois, Urbana-Champaign. In 2015 he founded Risk Management Levers, Inc., a consulting firm focused on risk management (including cybersecurity, enterprise risk management and reputation risk) and acquisition integration. Mark previously enjoyed a diverse career at BMO Financial Group, holding a variety of executive risk management and business leadership roles. Mark graduated from the University of Illinois, earned an MBA in Finance from The University of Chicago Booth School of Business, and is a CPA. He is currently earning his Cyber Security Management Graduate Certificate from the University of Virginia and was recently recognized as a National Association of Corporate Directors (NACD) Governance Fellow