CSX™
CYBERSECURITY NEXUS

The Cyberresilient Enterprise: What the Board of Directors Needs to Ask

Abstract

As enterprises strive to gain value by leveraging technology, the risk associated with digital business is increasing. Theft of personal information and private business information, misappropriation of resources, denial of service, and cybertheft are becoming commonplace, affecting large and small enterprises. Isolated approaches to information security, business continuity and incident response are a thing of the past; today, the urgency of providing continuously available services for customers and business partners in the digital economy requires enterprises to become resilient. A resilient enterprise protects itself from attack, but also recognizes that defense is not the end-all. A resilient enterprise needs to connect protection *and* recovery to the mission and goals of the enterprise, implementing integrated programs in order to provide sustainability of essential services. Board members need to evaluate the operational risk inherent in digital business and direct management to ensure that the enterprise is more than just protected—it is resilient.

ISACA®
Trust in, and value from, information systems
www.isaca.org/cyber

Key Insights

- The National Association of Corporate Directors recommends that "boards need to ensure that management is fully engaged in developing defense and response plans" and warns that to do otherwise is to place the enterprise's core assets at risk.[1]
- According to a recent Ponemon Institute study,[2] it took enterprises 170 days, on average, to detect an attack by malicious outsiders and 259 days when insiders were involved in the attack.
- Cyberresilience is the ability of an enterprise to anticipate, withstand, recover from, and evolve to improve capabilities in the face of adverse conditions, stresses or attacks on the supporting resources it needs to function.[3]

Given the nature of digital business and the value driven by the use of technology to meet stakeholder needs, the following questions may be appropriate for the board to ask:

- Is sufficient attention given to the ability to defend against intrusions as well as the ability to recover and restore essential functions and services?
- Is the board routinely informed about the potential material operational risk and risk mitigation strategies as well as incidents that could impact the brand?
- To what extent have essential services and functions been identified and programs implemented to provide for their resilience in the event of a disruption or cyberincident?

[1] National Association of Corporate Directors, *Cyber-Risk Oversight Handbook*, 10 June 2014, *https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688*

[2] Ponemon Institute, *2014 Global Report on the Cost of Cyber Crime*, *https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf*

[3] Bodeau, Deborah J.; Richard Graubart; *Cyber Resiliency Engineering Framework*, The MITRE Corporation, 2011, *www.mitre.org/sites/default/files/pdf/11_4436.pdf*

Introduction

Cyberincidents and the losses associated with these incidents have increased year after year, raising awareness among boards of directors and executives of the need for cyber risk governance and management. In a June 2014 speech at the New York Stock Exchange, Commissioner Luis A. Aguilar of the US Securities and Exchange Commission pointed to the increasing number and severity of cyberattacks and noted the unacceptable damage these attacks have inflicted on consumers and the bottom line for those who have been victimized.[4] While implementing risk management programs is a management responsibility, board members and audit and risk committees of the board need to take oversight responsibility to ensure that plans are complete and their implementation appropriately protects the organization.

The risk posture of enterprises is much different today due to the tight integration of information and communication systems into the fabric of operations and the markets that are served. When coupled with technical risk and the potential for intrusion and compromise, enterprise risk management necessitates the implementation of new approaches to protection and response. Information technology is an essential part of how business is conducted, and cyberprotection is no longer a technical issue; it is a business issue requiring board attention.

What threatens the enterprise today is very different from threats that existed just a few years ago. For example, if a potential virus infection was detected then, management could implement software to detect and eradicate malware. In response to social engineering, staff could be educated so they knew not to open suspicious attachments and understood how to respond to questionable email messages or phone calls. For each seemingly technical threat, there was a technical response.

Today, however, it is not enough to focus solely on technical threats and technical solutions. Enterprises face persistent attacks that exploit weaknesses in a more systemic manner. Attackers need to be successful only once to penetrate the enterprise, while security measures must be effective each and every time, regardless of the method of attack.

While cyberattackers still employ technical and social mechanisms that have been in use over many years, the difference is that today's attackers are persistent and the attack techniques they employ include advanced methods. Attackers are focused on and capable of circumventing controls or finding the weakness that enables them to steal trade secrets and personally identifiable information (PII), commit fraud, or otherwise capture precious resources. Implementing technical controls, prevention and detection are no longer sufficient. Today, cybersecurity now needs to be addressed in a more holistic manner. Building higher defensive walls and installing defense-in-depth solutions are no longer sufficient to prevent criminal intrusions and compromise.

In the digital economy, successful enterprises are those that can anticipate threatening events, continue essential activities despite adverse conditions and restore mission-critical functions quickly. Even more important, the successful enterprise has the ability to evolve so that the impact of potential and actual incidents is minimized. These capabilities encompass more than is traditionally associated with information security, disaster recovery, business continuity and crisis management. Individual protective capabilities and plans need to be integrated into a more holistic approach to protection. The ability to protect the enterprise from cyberhazards and sustain essential functions is the foundation of the cyberresilient enterprise.

Because of the rapidly changing integration of digital solutions into emerging and traditional business functions, the board needs to be confident that it

[4] Aguilar, Luis A.; "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," 10 June 2014, *www.sec.gov/News/Speech/Detail/Speech/1370542057946*

has the necessary information to evaluate, direct and monitor management's programs and practices.

Here are some questions that may be appropriate for the board to ask in order to gain this assurance:

- Is the board equipped with the right competencies to understand cyber-related risk and determine if management is taking appropriate action?
- Does the enterprise have the ability to detect changing threat conditions and understand the potential enterprise risk associated with these changes?
- Is the board sufficiently informed about changes to the business's use of technology and associated operational risk to exercise its responsibility?
- To what extent do information and cybersecurity programs align with business requirements?
- Do information security and business line leaders collaborate in understanding risk and appropriate technical solutions?
- Does the board get direct feedback from the chief information security officer or some equivalent officer who can explain in "business and strategic terms" the cyber risk and controls approach?

Cyberresiliency

Information and communications technologies are an essential part of how enterprises operate and how business is done. According to Internet World Stats, more than three billion people are now connected to the Internet.[5] Ericsson's CEO has estimated that by 2020 there will be as many as 50 billion connected devices.[6] The combined forces of mobile technology, cloud computing, social media and big data are fueling dramatic social and economic changes. Mobility and anywhere-access to information and services are creating opportunities for businesses to enter markets with new products while also innovating how existing products are offered to consumers. In 2012, The Boston Consulting Group estimated that by 2016 the cyber-related economy will reach US $4.2 trillion in the G20 economies; that means that if the cyber-related economy were a national economy, it would be the fifth largest in the world.[7] Boards cannot ignore the opportunity this market represents. Neither can boards fail to ensure that adequate and proper plans are in place to enable the enterprise to avoid attacks and respond to and recover from inevitable cyberincidents. The National Association of Corporate Directors recommends that "boards need to ensure that management is fully engaged in developing defense and response plans" and warns that to do otherwise is to place the enterprise's core assets at risk.[8]

[5] Internet World Stats, 2014, *www.internetworldstats.com/stats.htm*

[6] Ericsson, "CEO to shareholders: 50 billion connections 2020," 13 April 2010, *www.ericsson.com/thecompany/press/releases/2010/04/1403231*

[7] The Boston Consulting Group, *The Internet Economy in the G-20*, 19 March 2012, *https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/*

[8] National Association of Corporate Directors, *Cyber-Risk Oversight Handbook*, 10 June 2014, *https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688*

While the cyber-related economy is experiencing double-digit growth, losses due to cybercrime are continually increasing. A 2014 study revealed that the mean annualized cost for cybercrime among its 257 benchmarked enterprises was US $7.6 million per year. Some enterprises in the study reported losses reaching as high as US $61 million.[9] These losses are the direct result of the compromise of PII, theft or redirection of assets, fines, and legal costs. Less visible can be the loss of reputation and good will, damage to the brand that has been built over many years, and the costs related to recovery following the incident.

While boards are taking effective action in monitoring, directing and evaluating cyber-related programs, less attention is typically paid to recovery planning. Boards do need to consider the avoidance of incidents through protective measures, but that is not all that should be on their agendas relative to cybersecurity. They also need to recognize that cyber-related activities are an integral part of the business and, therefore, resiliency is equally essential, adds value to the enterprise, and is deserving of their attention, especially because stealthy and persistent attacks are becoming more prevalent.

Cyberresilience is the ability of an enterprise to anticipate, withstand, recover from and evolve to improve capabilities in the face of adverse conditions, stresses or attacks on the supporting resources it needs to function.[10] This is greater than the combination of information security and business continuity planning. To be resilient, a holistic approach to understanding and prioritizing business risk and implementing risk management activities needs to be integrated into day-to-day operations across all business functions. A resilient enterprise knows which information and communications systems are mission-critical and has taken the steps to prevent disruption while also recognizing that total protection is impossible. Knowing that cyberincidents still occur even in well-defended enterprises, boards of resilient enterprises ensure that policies and practices are implemented to reduce damage in the event of an incident, effectively manage the incident and improve by learning from each incident.

Given the nature of digital business and the value driven by the use of technology to meet stakeholder needs, the board needs to be assured that management's plans not only address defense, but also ensure that the enterprise is resilient. The following questions may be appropriate for the board to ask:

- Is sufficient attention given to the ability to defend against intrusions as well as the ability to recover and restore essential functions and services?
- Is the board routinely informed about the potential material operational risk and risk mitigation strategies as well as incidents that could impact the brand?
- To what extent have essential services and functions been identified and programs implemented to provide for their resilience in the event of a disruption or cyberincident?

[9] Ponemon Institute, *2014 Global Report on the Cost of Cyber Crime*, *https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf*

[10] Bodeau, Deborah J.; Richard Graubart; *Cyber Resiliency Engineering Framework*, The MITRE Corporation, 2011, *www.mitre.org/sites/default/files/pdf/11_4436.pdf*

Defining Cyberresiliency Priorities

A cyberresilient enterprise connects cybersecurity priorities with the core mission and goals of the enterprise. Stakeholders and their needs and interests are defined and prioritized, and this information guides investments in cybersecurity, business continuity and incident recovery activities. Cyberincidents threaten both the assets and the essential activities of the enterprise. The objective of cyberresilience is to ensure that critical processes continue to be available at an acceptable level even during a threatening incident. To accomplish that objective, it is essential for the enterprise to understand and prioritize stakeholder needs, identify the core business processes that are essential to meeting the mission and goals of the enterprise, and understand the potential impact a cyberevent will have on critical business enablers.

Enterprises exist to create value for stakeholders, including owners, shareholders, employees, business partners, and the customers and clients that the enterprise serves. Cyberincidents disrupt value creation by:

- Threatening the ability of the enterprise to continue to serve clients and customers
- Impacting critical business relationships
- Creating legal and regulatory challenges
- Impeding future opportunities when sensitive plans, designs and process information are compromised
- Eroding public confidence and customer good will when private personal information is disclosed

Value creation is a governance objective, as it is core to the purpose of the enterprise. Anything that threatens the ability of the enterprise to create value must be a priority for the board. Value, as defined in *COBIT® 5 for Risk*, involves a balance among benefits realization, risk optimization and resource optimization.[11] The promise of value that digital opportunities present needs to be balanced with the risk that is an inherent part of these opportunities. Cyber risk that is considered only in terms of technology is not connected to the enterprise's quest for value. As a result, risk may be isolated from business goals and objectives, and risk impacts to the enterprise may be miscalculated. The failure to connect cyber risk to business processes and plans may produce several negative outcomes relative to critical value-producing activities and programs: They may be disrupted, they may no longer be able to maintain an acceptable level of performance, or they may not be recoverable within the needed time frame.

An effective IT governance framework can help mitigate some of the risk. The chief audit executive (CAE) may use a maturity model (i.e., COBIT Process Assessment Model)[12] to communicate to the board and senior management the current status of the IT governance environment. By assessing the enterprise's IT governance maturity level, senior management—with support and direction from the board—can begin to modify and/or implement practices, policies and procedures that will assist the enterprise with IT governance optimization.

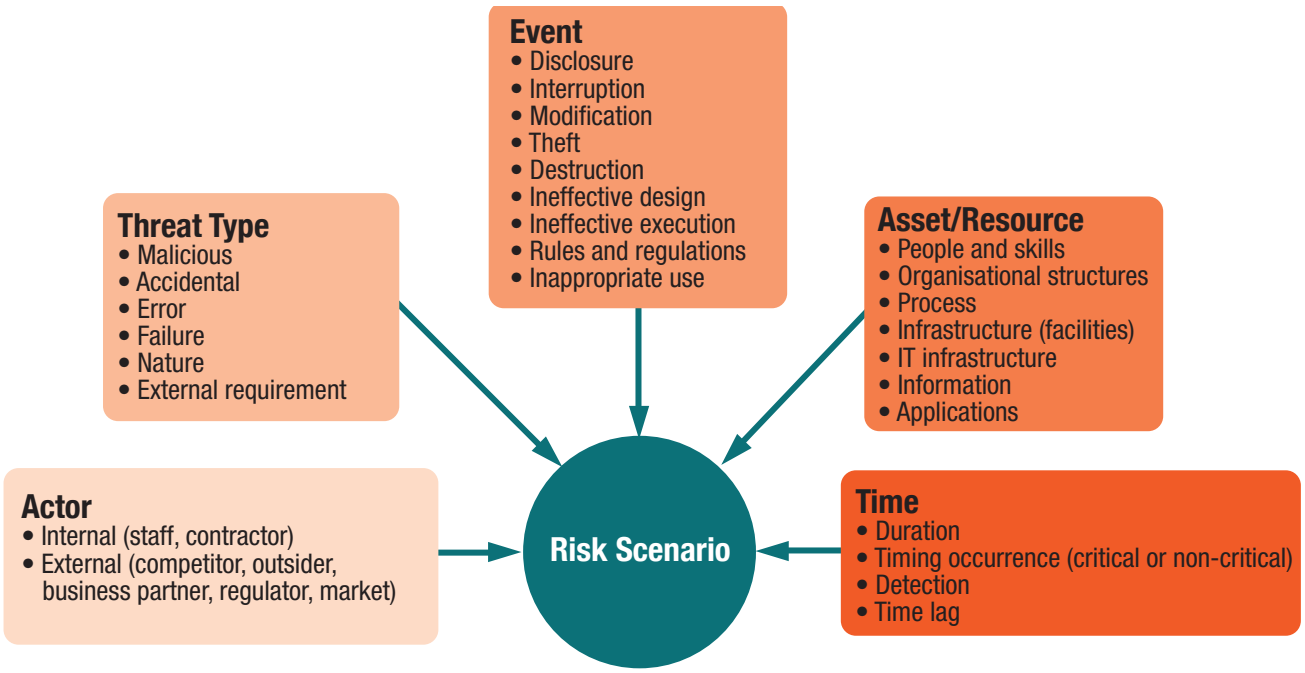
[11] ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

[12] ISACA, *Process Assessment Model (PAM): Using COBIT® 5*, USA, 2013, *www.isaca.org/COBIT/Pages/COBIT-Assessment-Programme.aspx*

Risk optimization requires the board to understand management's plans and activities to balance risk acceptance and avoidance within the context of enterprise goals, strategy and objectives. The board needs to approve the risk-reward balance that is defined in terms of risk appetite. The balance point between risk acceptance and avoidance needs to be communicated across the enterprise so it is part of the planning and administration of cyber-related business activities.

Risk scenarios are often used as an aid to ensure that risk is identified and the balance between acceptance and avoidance is maintained. Risk scenarios use business terms to describe the effect a risk can have on the achievement of an enterprise's objectives, based on an understanding of the origin, nature, characteristics, resources impacted and time duration of a risk incident.[13] **Figure 1** contains a generic description of the contents that should be included in a risk scenario.

FIGURE 1 Risk Scenario Contents



Source: ISACA, *COBIT® 5 for Risk,* USA, 2013, figure 36

[13] ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

Identifying cyber-related business risk and integrating it into business planning and administration through scenario planning depend on defining critical business processes, understanding what is minimally required to continue these processes, and determining the time frame within which restoration of full capability is essential. Understanding risk through the use of risk scenarios also connects the different functions within the enterprise because, in the modern enterprise, core functions and capabilities essential to meeting stakeholder needs cross organizational boundaries.

As the board looks to meet stakeholder expectations and grow the business, identifying risk and implementing risk programs need to be weighed carefully. The following questions may be appropriate for the board to consider in this context:

- Are business impact assessments and scenario planning exercises used to document the criticality of business processes and services? Are they updated to reflect changing requirements as new technology-dependent services and products are introduced or enhanced?
- In considering digital products and services, to what extent are the desired goals and benefits balanced with an understanding of risk?
- Have formal methods been adopted to provide a balanced approach to business planning and risk identification and response?

Protection and the Cyberresilient Enterprise

In 2014, ISACA and The Institute of Internal Auditors Research Foundation issued a joint publication, *Cybersecurity: What the Board of Directors Needs to Ask*, which stated that cybersecurity is an imperative for the board and recommended that board members demand information and insight to help them secure the future of the enterprise.[14] Board members need to be informed of business activities and cyber risk so they can exercise their responsibility to evaluate and direct management, which in turn guides and implements cyberprotection programs.

An important element of achieving cyberresilience is the ability to implement protective measures that are consistent with the risk/reward balance approved by the board. Cyberdefense is not a one-time activity. Cybersecurity strategies and programs must adapt to the changes that arise from the enterprise's evolution, which is a natural result of its incorporation of new technologies, delivery of new products and services, and engagement with new partners. As the threat landscape changes, risk scenarios need to be revisited and security practices modified to address new priorities. Maintaining an effective cybersecurity posture requires constant attention and the ability to understand current conditions and the capabilities that will be required as a result of change. Given the complexity of cyberprotection and the need to respond to the application of new and emerging technologies to business issues, it is important for the enterprise to employ a structured approach to cybersecurity program design and management.

[14] The Institute of Internal Auditors Research Foundation, ISACA, *Cybersecurity: What the Board of Directors Needs to Ask,* 2014, *https://www.theiia.org/bookstore/product/cyber-security-what-the-board-of-directors-needs-to-ask-download-pdf-1852.cfm*

In July 2015, The US National Institute of Standards and Technology (NIST) released an update to *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). The framework acts as a guide for enterprises to develop and maintain programs that integrate solutions intended to address cyber risk as part of the enterprise's risk management processes.[15] The framework draws upon well-established guidance such as *COBIT® 5 for Information Security* and international security standards such as ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements* to provide small to large enterprises with common principles and best practices that are internationally recognized to improve protection and resilience in the face of continued risk. The benefit in using *COBIT for Information Security* or the NIST Cybersecurity Framework is that they ground the enterprise in international best practices and standards and provide a defensible position that demonstrates that a complete and holistic approach has been implemented.

As a business imperative, cybersecurity needs to provide for the proper governance of the function, the ability to prioritize programs for the greatest impact, and technical and administrative elements required to design and implement the cybersecurity architecture. In defining the protection program, consideration must be given to the variety of incidents that can erode value and impede the delivery of essential services. Protection also requires the recognition that attacks can come from trusted sources, including service providers and business partners.

While many cyberincidents are technical in nature, people can also be the cause of or significantly contribute to an incident. The loss or compromise of PII can result from employee error or omission—perhaps something as simple as failure to protect physical documents or loss of a mobile device.

The changing nature of the digital world and threats to enterprises create a need to think about protection in a different manner. The following questions can help the board to ensure that an appropriate level of protection—a level that addresses the wide variety of avenues for attack and compromise—is provided:

- Have formal and structured methods been established for implementing and managing the cyberprotection program in a way that is consistent with established frameworks or standards?
- Are protection programs for defense and incident detection integrated into a more holistic approach to response and recovery?
- Does the protection program address security in a holistic manner, considering technical risk as well as incidents that can arise from errors and omissions by internal sources and third parties?

[15] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2015, *www.nist.gov/cyberframework/*

Sustainability and the Cyberresilient Enterprise

The ability to protect the enterprise from intrusion is only part of what is required to ensure that stakeholder needs continue to be met and the expected value of digital business is consistently delivered. Also integral to continued success is providing for the continuity and recoverability of essential services and processes, in spite of threats such as digital harassment in the form of denial-of-service attacks, intrusions, thefts and the compromise of system integrity. Prudent enterprises prepare to avoid incidents but they also implement disaster recovery and business continuity plans. Their need is twofold:

1. Respond when an incident is detected.
2. Have an integrated capability that connects protection with detection, response, recovery, and more important, the continuance of core services and functions.

The resilient enterprise ensures that it can achieve its strategic goals by identifying and prioritizing areas of operational risk and sustaining core services when risk is realized. As an integral part of identifying strategic goals and potential risk, the resilient enterprise faces challenges as they occur and is able to return operations to normal as quickly as possible.[16] However, disaster recovery and business continuity may focus mainly on the *recovery* of technical capabilities and may not consider holistically the value-producing environment on which the enterprise depends. Resiliency requires all activities, programs and processes—from the specification of enterprise goals and stakeholder needs, through operational risk identification and protection planning, to incident detection and recovery and awareness training—to be part of an integrated and holistic enterprisewide approach.

Nearly all enterprises are likely to experience an incident from significant to benign at some time, regardless of their investment in protection. An enterprise can be specifically targeted or can be victimized when a partner or service provider falls to a cyberattack. A cyberincident can arise from errors or omissions of employees, or an attack may result from newly discovered vulnerabilities or a failure to patch systems. The multiple paths available to attackers make it impossible to guarantee protection.

Protection must be balanced with continuous monitoring of the environment and, in particular, essential systems and networks so anomalies and incidents are detected quickly. It is not uncommon for many attacks to go undetected for months and then come to management's attention only when too much damage is done. Unfortunately, it is even more common for victims to become aware only when they are notified by an enterprise or someone impacted by the same attack. At this point, losses are probably material. Such a delay in detection and response is difficult to explain to shareholders, partners and customers. How could a compromise of such significant magnitude not have been detected much earlier? According to a recent Ponemon Institute study, it took enterprises 170 days, on average, to detect an attack by malicious outsiders and 259 days when insiders were involved in the attack.[17]

Incident response is crisis management. The level of crisis is related to what is at risk, namely the reputation and brand of the enterprise, financial loss, and the trust and loyalty of stakeholders. Stakeholders are likely to consider the enterprise's behavior during a cybercrisis as indicative of the quality of its leaders and its values. A cyberincident's long-lasting impact may have more to do with how well the incident appeared to have been managed than with the number of records compromised or value lost.

[16] Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; Young, Lisa R.; *CERT® Resilience Management Model, Version 1.0,* Software Engineering Institute, May 2010 *http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479*

[17] Ponemon Institute, *2014 Global Report on the Cost of Cyber Crime, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf*

Communication is potentially even more important than other elements of incident management and recovery. Cyberincident management requires broad participation across the enterprise, incorporating technology and policy expertise. Cyberincident-related communication must be strategic, purposeful and inclusive. Transparency with internal and external audiences is key, as almost any attempt to conceal the truth is certain to be interpreted negatively.

Cybercrises are often characterized as starting with the detection of the incident and concluding with the eradication of the malware or compromised software. However, intrusions are often experienced even after the supposed return-to-normal point. The cyberresilience program needs to cover the need for caution in declaring the end of the incident.

Cyberincidents can quickly become a crisis situation unless there is early detection and effective response. The following questions can help the board to ensure that appropriate and effective detection and response capabilities have been implemented:

- Is incident detection sufficiently integrated with response and recovery to make the enterprise resilient?
- Have incident/crisis management experiences demonstrated that the enterprise has the capability to be resilient? Have these incidents been used to enhance resilience capabilities?
- Are detection capabilities sufficient to identify anomalies that could indicate a cyberintrusion or attack?
- Has the appropriate management structure been implemented to ensure an effective response capability?
- Has a crisis communication capability been implemented and integrated into response planning?
- Are all stakeholders and their needs identified and considered when developing incident response plans?
- Has incident response been recently practiced and lessons learned used to update and refine the incident response program?

Summary

While the value of competing in the digital economy is evident, it is also clear that cybercriminals can compromise even the best of security defenses. The persistent nature of attackers ensures that they will find an avenue of compromise and, once they penetrate defenses, they will be able to expand their access and achieve their goals. The cybercriminals' advanced attack techniques and use of methods for which there is no known protection (the zero-day vulnerability) may render enterprises defenseless. The value of digital business and the threat of compromise require boards to ensure that effective programs are in place not only to defend the enterprise, but also to detect and respond to incidents and expeditiously recover essential services and functions. Regulatory bodies, legislators and courts are recognizing the need for enterprises to provide effective governance and management for cyberprotection and sustainability. Effective governance by boards is essential to ensure that stakeholder needs and priorities are known and considered when developing protection programs to create the truly resilient enterprise.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: www.isaca.org

Provide feedback:
www.isaca.org/cyberresilient

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
ISACA (Official),
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.

Reservation of Rights

ACKNOWLEDGMENTS

ISACA wishes to recognize:

Lead Developers

Ron Hale
Ph.D., CISM,
ISACA, USA

Project Contributors

Todd J. Fitzgerald
CISA, CISM, CGEIT, CRISC,
CISSP, CIPP/E/US, PMP,
Grant Thornton International, Ltd., USA

Steve Mar
CISA, CSFA
IT Audit Director, Nordstrom, Inc., USA

Laurie E. McDonald
CISA, CISM, CRISC, CIA, CPA,
Computershare, USA

Jason Philibert
CIA, CFE, CRMA,
TriNet Group, Inc., USA

James Reinhard
CISA, CIA, CPA
Simon Property Group, USA

Daniel L. Ruggles
CISM, CGEIT, CRISC, CISSP, CMC, CSM, CSPO,
PMP, PMI-ACP,
PM Kinetics LLC, USA

Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC,
INTRALOT S.A., Greece, International President

Rosemary M. Amato
CISA, CMA, CPA,
Deloitte Touche Tohmatsu Ltd., The Netherlands,
Vice President

Garry J. Barnes
CISA, CISM, CGEIT, CRISC, MAICD,
Vital Interacts, Australia, Vice President

Robert A. Clyde
CISM,
Clyde Consulting LLC, USA, Vice President

Theresa Grafenstine
CISA, CGEIT, CRISC, CPA, CIA, CGAP, CGMA,
US House of Representatives, USA, Vice President

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM,
CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA,
GCIH, GSNA, GCFA,
ATD Solution, Singapore, Vice President

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA,
APIT Consultoria de Informatica Ltd., Brazil, Vice President

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP,
WhiteOps, USA, Vice President

Gregory T. Grocholski
CISA,
SABIC, Saudi Arabia, Past International President

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA,
Queensland Government, Australia,
Past International President

Robert E Stroud
CGEIT, CRISC,
USA, Past International President

Zubin Chagpar
CISA, CISM, PMP,
Amazon Web Services, UK, Director

Matt Loeb
CAE,
ISACA, USA, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC,
Versatilist Consulting India, Pvt., Ltd., India, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP,
BRM Holdich, Australia, Director