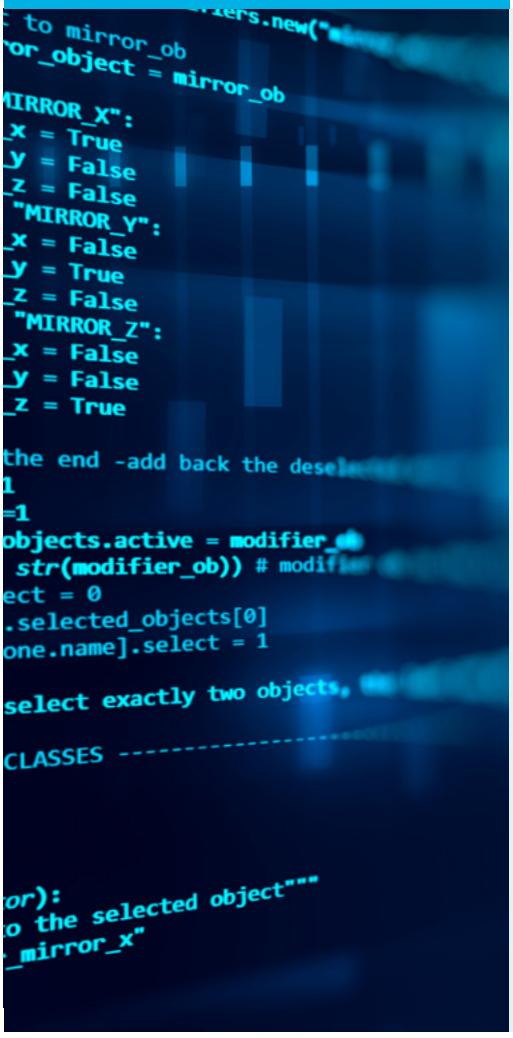
White Paper

Addressing the Whole-of-Enterprise Threat

By Samuel Sanders Visner, Senior Vice President and General Manager, Cybersecurity, ICF, and Jeff R. Hunt, Partner, PulsePoint/Olson, an ICF Company



Introduction

Recent cybersecurity incidents at Sony, a German steel factory, Target, Anthem, and elsewhere highlight the need for better preparedness and a more coordinated response. The information technology environment in which we operate is dynamic. Threats change every day, as do the architectures on which we depend. Cyber-criminals and foreign intelligence services conduct constant reconnaissance against current and potential targets. They accrue "exquisite intelligence" regarding those targets. They have greater and timelier knowledge—in some cases more about a target's network topology and administration than the target itself possesses. Even the configuration of an enterprise's IT architecture is not fixed: New users are added. New applications are brought on line. Workload is shared, and shifted, dynamically among different cloud providers.

Even more nettlesome: We struggle to attain effective cybersecurity in IT environments no one enterprise controls. Consider today's retailers. Many outsource their customer intelligence and outreach at the front end of their business while sharing responsibility with suppliers for supply chain components (the back end) of their business. For their supply chains, some companies rely on business-to-business exchanges connected with other companies. IT infrastructures serve customers and subcontractors of all participating businesses. In other words, the IT environment today's enterprise seeks to secure is not contained to that enterprise. It is, by definition, **non-containable.**

Consequences of Cyber-Attacks

The consequences of today's serious cyber-breaches also are non-containable. The porous or shared nature of today's information infrastructures reduces the likelihood that information about a breach will be known first by the targeted enterprise. In fact, the breach in 2013 against a leading retailer was revealed by a blogger. Vulnerabilities created or exploited by an adversary may be detected by others, some of whom may be keen to embarrass the enterprise being exploited or attacked. Today's critical infrastructure, also known as the "internet of things," transforms computer peripherals into more and more devices such as pipeline valves, railway switches, and power nodes. Cyber-attacks against critical infrastructure and these devices can have physical consequences, difficult if not impossible to conceal. The nature of today's connected world allows unvetted and unfiltered news to travel far more swiftly than existing incident response plans can be put into effect. Even 30 years ago, before the Internet and social media, Soviet efforts to conceal and "spin" the Chernobyl disaster were thwarted by a French imaging satellite and radiation detectors in the West. Today, in the era of Twitter and instantaneous transmission of news, the challenge is orders of magnitude greater.

In addition, the effects of breaches may be felt in parts of an information infrastructure on which an enterprise depends, including its supply chain, but does not fully control. Without incident response plans shared among partners, an enterprise would be foolhardy to believe that it can constrain the flow of information about serious cybersecurity problems.

Other Aspects of Non-Containability

Non-containability has other aspects. Regulated industries, such as financial services and health care, face regulatory requirements. Failure to heed requirements can be costly. As envisaged by the 2014 Framework published by the National Institutes of Standards and Technology (NIST), the creation of sector-specific cybersecurity standards will publicize best practices. In the wake of serious intrusions, shareholders, customers, suppliers, boards, and others will likely demand to know: Did the enterprise and Hawaii—have 34 percent of the installations. Thus, the operational experience with distributed solar PV on the bulk power grid has been fairly limited. apply these best practices and standards? If not, why not? Companies comprising the defense industrial base, whose operations are considered to be of national security importance, are required to report cybersecurity problems to the U.S. Department of Defense.

Here is another trenchant reality: Whether the standards that result from the NIST framework and other efforts are mandatory or voluntary, their very existence and widespread adoption will place every enterprise to which they pertain under additional scrutiny. They may become the "standard of care" for civil liability.

These are hard problems, but they are not insurmountable.

Perfect cybersecurity is practically impossible. Effective cybersecurity that allows an enterprise to maintain its business and mission while recovering affected operations can be achieved. Cybersecurity incidents are likely to become public knowledge. Those organizations faced with the response to and the consequences of such incidents must account for themselves in public. The adoption of best practices is no longer optional.

Required Knowledge Base

Enterprises subject to cyber-attack and exploitation must become more self-aware. Every enterprise should know key information about its operations and recognize that adversaries certainly will do whatever possible to know the same information. Enterprises must regain—and keep—their information advantage. To do so, they must gather and constantly renew this knowledge constantly. Five key areas of content knowledge and understanding are described more fully below:

- Inventory of valuable information
- Network knowledge and chain of responsibility
- Cybersecurity policy
- Vulnerability assessment
- Emergency planning

Inventory of valuable information—First, any enterprise that relies on information and IT (whatenterprise does not!) must create and maintain an inventory of the information deemed mostvaluable, the compromise or destruction of which would be most damaging. For some enterprises,this information relates to financial or customer data; for others, vital intellectual property forms thecore of their business. For critical infrastructure owners and operators, the data may be central to managing, operating, and securing the infrastructure.

Network knowledge and chain of responsibility—Second, enterprises should understand their own networks. They must understand them from a logical and topological perspective. How is it built? How much do we control? How much do we share? What do we know about it? What do we know about the cloud providers to whom we have entrusted our operations? How well do we understand the topology of the networks on which we rely, particularly in a world in which we will allocate workload dynamically to more than one cloud provider?

And they must understand the networks from an administrative perspective. Who is responsible for what in our enterprise? Who has administrative privileges? What are those privileges and when where they granted? Not surprisingly, some enterprises have a dim understanding of the cadre of people to whom administrative privileges have been given and from whom they should have been revoked.

Cybersecurity policy—Third, every enterprise should establish and maintain the best possible awareness of how its cybersecurity policy is applied and enforced. Have firewalls been maintained?

Are passwords being changed? What data loss prevention, intrusion detection, and other tools are in use? In other words, what is the overall state of the enterprise's governance, risk, and compliance vis-a-vis its own policies?

Vulnerability assessment—Next, every enterprise should work continuously to understand its vulnerabilities. In a world in which threats change frequently and networks are dynamic, periodic vulnerability and penetration testing must give way to continuous monitoring of networks for both vulnerabilities (ranging from poor selection of tools and techniques to their inadequate application) and penetration.

A variety of approaches exist to detect breaches. Research indicates that some breaches exist as much as a year before they are detected. This finding speaks to the need to adopt approaches that include analyses of logs to reveal unauthorized use of administrative privileges and the presence of malware as well as assessment of network behavior. The organization must compare actual behavior to the behavior expected with a good understanding of network composition and topology.

Emergency planning—Finally, every enterprise should practice emergency planning. How do we prepare for a cybersecurity emergency? Have we done what we could to prevent it? Are we in a good position to recover from such an emergency? Can we sustain our vital operations, even while our enterprise deals with the realities of a cyber-intrusion? Whom do we need to mobilize? Who needs to be informed?

This last element has two general areas of responsibility an enterprise must address, technical/operational and strategic communication. Doing so gives to the enterprise that does a special opportunity to *gain the upper hand when a cybersecurity breach occurs.*

First, an enterprise must plan for its technical/operational response. It must assess the extent of the compromise of systems and information and what recovery of their security requires. They also must determine the integrity of the information and systems affected by the breach. The enterprise should equip itself in advance with the resources or partners that can conduct the forensics investigation necessary to understand what happened, what is still happening, and how to keep it from happening a new Given that the breach may, and likely will, involve partners, this technical response may require coordination with other affected parties.

Other Considerations

An enterprise operating in today's non-containable environment should consider the need to work with regulators, suppliers, customers, boards, and others. Stakeholders must know that the situation's scope is being assessed and that the enterprise understands the stakes for itself and for them.

The need for effective response that encompasses an enterprise's operations and its reputation has never been greater, and it will only grow. Questions relating to privacy, financial impact, loss of intellectual property, and in the case of critical infrastructure, the public's safety will emerge and emerge swiftly. Strategic communication with stakeholders in a crisis environment requires crisis planning to sustain the confidence of those affected and to coordinate the response.

Today's cybersecurity planning and response tends to be fragmented organizationally. Chief information security officers (CISOs) assess logs for forensic data. Corporate information officers (CIOs) attempt to regain operational cadence. Chief financial officers (CFOs) ask if revenue and margin impairment is likely (and if so, how large might it be). General counsels consider liability. Chief communications officers (CCOs) try to distill a myriad of technical, regulatory, operational, and other information in a strategy with a coherent set of messages that limit reputational damage.

Such an approach leads inevitably to a fractured response, one in which information is inconsistent and actions are uncoordinated. Efforts to understand the nature, severity, and scope of an incident are overcome by the pace of public speculation regarding the incident. Such speculation may not be congruent with reality, but it may become the dominant narrative and come to define the organization in a way that causes lasting damage.

Essential Approach

A "whole-of-company" or "whole-of-enterprise" approach is essential to cybersecurity planning and response. CISOs and CIOs, CFOs, CCOs, chief marketing officers (CMOs), general counsels, and line-of-business leaders should convene periodically with the explicit support of the chief executive officer. They should build structured plans that define areas of responsibility and the coordination mechanisms for ensuring a consistent response. This response must regain business and mission operations. It must restore the upper hand regarding an enterprise's reputation and be coordinated and consistent in reporting to regulators, the board, and others. Because of their overarching responsibilities for an enterprise's financial performance and reputation, CFOs and CCOs can play an important role in bringing together this executive team. They should be core components of such a team and serve as advocates for a coordinated response that encompasses the development and sustained activities of the team.

Conclusion

Adoption of a whole-of-enterprise approach requires real work and coordination well before a cybersecurity breach occurs. That work pays dividends. Having such an approach in place can provide an enterprise a matchless opportunity to recover swiftly, communicate clearly, and coordinate effectively. The enterprise can preserve vital information, sustain business and mission operations, and limit damage to, and perhaps enhance, an enterprise's reputation. In today's non-containability world, an enterprise should do no less.

About ICF

ICF (NASDAQ:ICFI) is a leading provider of professional services and technology-based solutions to government and commercial clients. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 65 offices worldwide. ICF's website is **icf.com**.

About the Authors

Samuel Sanders Visner is a Senior Vice President and the General Manager of Cybersecurity at ICF. The former Chief of Signals Intelligence Programs at the National Security Agency, he is an adjunct professor of Science and Technology in International Affairs at Georgetown University.

Jeff Hunt is one of the world's leading experts in crisis preparedness and communications, having worked with Fortune 100 companies around the world. He has counseled CEOs and boards in times of serious crisis, including IBM, Penn State, DuPont, AT&T among many others. He is currently actively involved in helping Japan's, TEPCO, recover from one of the worst nuclear disasters in Fukushima, following the great Japan earthquake and tsunami.

For more information, contact:

Samuel Sanders Visner
samuel.visner@icf.com +1.703.225.5860

Jeff Hunt
jeff.hunt@icf.com +1.512.426.6782