Shifting Risks and IT Complexities Create Demands for New Enterprise Security Strategies

Sponsored by: Booz Allen Hamilton
Simon Ellis  Christina Richmond
February 2014

IDC OPINION

The Challenge

"... is to develop a comprehensive view of every threat that's hitting our environment ... and that's a real change [in strategy]. ... It's about partnering with the right organizations, getting the right tools, and making sure we have the right people. That's a significant challenge."

(Global Financial Services Firm)

Today's businesses operate in an environment of greater collaboration, transparency, and scrutiny than at any time in history; and they are both sending and receiving more information than ever before. Indeed, the ability to compete in this current business environment requires these companies to effectively receive, analyze, and then disseminate information to suppliers, customers, and even consumers in easily accessible and flexible ways, often with very short lead times. As important as this information flow is to the performance of the business, it creates an enormous challenge for IT and information security organizations to effectively maintain data integrity and security.

In a recent research study, IDC interviewed information security executives across five industries: financial services, federal government, large supply chain manufacturing, oil and gas, and pharmaceuticals/life sciences. The goal of the study was to better understand the evolving threat landscape from their perspective and its impact on risk and security strategies. Through these interviews, IDC confirmed that the dynamic, complex threat landscape in which these industries operate is causing security executives to reevaluate their roles and responsibilities as well as the skills, tools, and partners necessary to keep their businesses safe from harm. Central to the issues uncovered is the reality that firms can no longer think in terms of the react and defend capabilities delivered by on-premise, signature-based technologies. They must instead adopt a more complete "security life cycle" approach with an emphasis on the ability to predict and prevent. This requires clearly understanding the threat and potential impact of a security event before it impacts the organization through the use of behavioral, emulation, and sandboxing technologies necessary to prevent infection and minimize risk. Increasingly sophisticated and advanced threats require a complete set of decision management capabilities based on discovery, detection, intelligence, savvy interpretation, and enterprisewide integrated execution. Furthermore, this approach requires end-to-end threat analytics and an understanding of the
business issues that span loss of data, legal considerations, regulatory requirements, brand, customer loyalty, and more. Security executives – particularly chief risk officers (CROs) and chief information security officers (CISOs) – must be able to articulate these issues at all levels of the enterprise and across all core lines of business.

The future enterprise security model goes far beyond mere compliance strategies, with their basic data loss prevention, datacenter perimeters, and remediation methods, to include advanced threat detection, protection, and prevention. Security executives are beginning to recognize that getting to this future state requires broader, deeper expertise than is currently available within their organizations, which are replete with security complexity. Indeed, it may well be that the current security challenges exceed reasonable internal "core competencies" and that external partners become necessary.

IN THIS WHITE PAPER

In this white paper, IDC discusses the complex security threat landscape, the changing role of the CISO and CRO, and the consequential need for a broad-spectrum, end-to-end security partner and service provider. The right partner can share risk management, recommend best practices, and facilitate a full security posture that is highly integrated, agile, adaptable, and scalable for a rapidly evolving threat landscape.

SITUATION OVERVIEW

The Emerging Threat Landscape

IDC found that most executives who were interviewed believe that advanced attacks are on the rise, in terms of both frequency and sophistication. According to these executives, the attacks evade many of the established and proven detection methods in place today and can confound even the top security analysts. In addition, the threat landscape is so complex that many CISOs feel they can't keep up. CROs worry that increased security vulnerability can result in greater exposure to risk overall.

"The nature of [APTs] being persistent, they can hammer at things for long periods of time instead of trying to hit it all at once, like a classic virus, malware, or hacker ... "

(Global Pharmaceutical Manufacturer)

The impact of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks is described by respondents in terms that range from "diversionary nuisances" to "major initiatives." With respect to advanced persistent threats (APTs), a common theme of "uncertainty" emerged from the interviews. One pharmaceutical executive conveyed that he and his colleagues are "greatly worried" about APTs, while a bank executive said that his bank is being attacked daily by APTs. In the latter case, the bank executive said, "Anomalies are occurring that can't be explained and shouldn't exist because policy and practice prevent them from happening, but they are happening." Worse, upon detection, APTs morph into something else. The new norm for security executives seems to be "waiting for the other shoe to drop," and this condition puts intellectual property (IP), monetary assets, and even business viability at high risk.
The perpetrators of cyberattacks are compensated for stealth and persistence by individuals, corporations, and nation-state entities. Further, threats have expanded into new forums. IDC sees threats and vulnerabilities in several new areas, including attacks on:

- Social media and mobile devices
- Employee-owned devices (bring your own device [BYOD])
- Private, hybrid, or public clouds, which demand significant IT transformation
- The Internet of Things, where every device – from manufacturing to automobiles and into the home – will eventually be connected to the Internet
- Software-defined networking (SDN) (an approach to networking in which control is separated from hardware and given to a software application called a controller), which will become a future challenge to IT security posture

It is no longer enough to bolt security devices onto an existing, often on-premise IT infrastructure and "tick the box" for compliance with an intrusion prevention device or firewall. Even advanced security information and event management (SIEM) solutions need bolstering. Enterprise security staff now are required to guard a pliable perimeter and monitor constantly changing elements such as big data, BYOD, cloud, employee mobility, and the Internet of Things. Software-defined networking, as it develops, will question network security at its foundation and may ultimately shift focus to application security. The cybersecurity environment is changing rapidly, and CISOs are tasked with showing their organizations how to ensure they are secure and protected.

**Targeted Attacks Increasing**

Cyberthreats create very real potential costs for an enterprise. These can range from millions of dollars in tangible costs to the difficult-to-track intangible impacts of brand damage, loss of reputation, loss of customers, and negative publicity. These intangible effects may not be seen right away or even clearly for some time after an event but can persist and have a significant longer-term impact.

According to IDC, the cost of targeted threats like DDoS and APTs ranges from $10,000 to more than $100,000 an hour in “damages” to the business. In many cases, the attacks lie undetected for hours or days, and sometimes even months, driving potential costs into the millions of dollars. One interviewee said that his bank’s clients lost approximately $6 million through fraudulent buyer activity; the bank absorbed approximately $250,000 of that cost. A pharmaceutical executive reported that while downtime is a concern, the real business impact is related to stolen IP. The theft of IP is a much more expensive breach and can result in losses of tens of millions to over a billion dollars. In this case, the executive estimated the brand and reputation damage to be hundreds of millions of dollars.

Media hyperbole moves us to believe that all attacks are created equally and that there is a set amount of cost by specific attack. Asked specifically about costs incurred during attacks, interviewees consistently could not quantify the cost impact in a
dollar amount. Most participants agreed that dollar amounts that are definitive across such broad, dynamic, and diverse threats are not calculated accurately and that they have been overblown by the media and opportunistic salespeople. However, this should in no way diminish the fact that attacks bring with them a hefty impact on both monetary and more intangible damage to brand and reputation. Just one successful attack can cause massive disruption and loss. The specter of unknown or hard-to-detect APTs moving around a network, in addition to known threats, is motivating CISOs to think differently about their roles and their responsibilities.

**New Role of the CISO and CRO**

Currently, a key responsibility of CISOs and CROs is to anticipate and mitigate attacks before they occur. To do this, CISOs need to understand sophisticated threats, gather threat intelligence, apply advanced analytics, deploy appropriate security tools, and know when and why to insource or outsource and how to talk about security in business terms. This paradigm shift cascades into day-to-day activities, such as managing staffing requirements, training employees, solving budgetary challenges, and evaluating security purchases and service engagements.

According to one executive IDC interviewed, employee education should be a top priority. Security leaders need to talk about the security dangers brought to the enterprise through BYOD and mobile applications deployed by the business units and by what one security executive bluntly called "dumb human behavior." He confessed that he has fallen victim to human error, which caused him to click on an infected link. This executive explained that his team blogs on a regular basis about the threats that are affecting staff members. CryptoLocker, for example, held some employees ransom, and they lost personal pictures and data at home.

Another example of the fundamental change occurring in security management is "shadow IT." This phenomenon occurs when business units purchase — without consulting IT — a platform or an application that they believe will advance the business through increased sales revenue or improved efficiency in their departments. The CISO has a choice to make at this juncture: become an obstacle to the business or work with the new purchase even if it presents greater risk to the security of the enterprise.

"The CISO and the CIO are becoming marketers to educate about security internally." (Global Pharmaceutical Manufacturer)

"... What [CISOs] really need is to develop social skills to be able to talk to the business, talk to people to get their interest, and then be a source of expertise and build trust ... The biggest skills change for me? It's not hard skills; it's the soft skills." (Global Pharmaceutical Manufacturer)

**Business First, Security Second**

"I would say that we heavily shy away from any business limiting for the sake of security. It's business first, and then what can we do to secure it afterward." (Supply Chain)
CISOs are receiving greater scrutiny from upper management and board members and need to be able to communicate the risks and costs associated with cyberattacks — not in back-office jargon that focuses on technical capabilities but in the language of the C-suite. If CISOs can do this, they can help their CEOs make swift, informed decisions in situations where minutes count. A trusted security partner can provide invaluable guidance to help CISOs embrace their new role quickly and effectively.

**Considering an External Partner**

Given the data security challenges faced by companies across multiple industries, and the growing sophistication of cyberthreats, it is incumbent on security and risk executives to decide how best to approach the problem. Is the best approach centered on internal resources or does it require engaging with a trusted third party — or is it some combination of both?

**The Challenge of Talent**

In consideration of how intelligence and analytics are shaping the future of security, CISOs and CROs must be thoughtful about the people who are executing their enterprise’s security strategy. An intelligence-based team has skills that go beyond IT security expertise: research, legal, communications, education, and management, for example. The challenge for CISOs is identifying the right mix of training and experience and nurturing desired behaviors: asking the right questions, intuiting the implications of data insights, respecting cultural nuances, following processes, communicating in an audience-appropriate manner, and so on. The extent to which the right people and the right skills exist within the business goes a long way toward determining how to best address the cybersecurity problems.

**Outsourcing Data Security**

If the conclusion is that internal resources are not adequate, or if the business determines that modernizing cybersecurity is simply not a core competency, then employing a trusted third party becomes a preferred option. Yet for many businesses, the fragmented nature of security-related external relationships can actually add to, rather than subtract from, overall data vulnerability. An emerging practice is to select a single, full-function external security partner in order to leverage the economies of scale that a managed security services provider (MSSP) gains from clients that span diverse customer segments and industries. An additional benefit to an engagement with an MSSP is the move from capital expense to a predictable monthly operational expense.

**Selecting a Third Party**

The actual selection process is varied and can depend upon a number of factors. Though cost always plays a part, it is less important in the consideration of a security partner because of the significant vulnerabilities involved in data and IT security breaches. Knowledge, experience, integration, and technology play a bigger role, which is discussed in more detail in the sections that follow.

A seasoned security partner can help CISOs and CROs hone and expedite their staffing activities with insights and guidance based on real-world experiences.
Supply Chain/Manufacturing

The increasingly distributed nature of the manufacturing supply chain is putting it a greater risk for data security threats and cyberthreats. While manufacturers are attempting to be more open and transparent with suppliers, contract manufacturers, customers, and even consumers, the very nature of this greater visibility leaves the supply chain open to data security breaches and cybercrimes. The very lifeblood of the manufacturers is in bringing new products to market, usually in partnership with various external suppliers, yet these partnerships, and the often casual ways in which critical information is exchanged, open up huge opportunities for cyberthreats. The difference between the success and failure of a product may well rest on the ability of the manufacturer to maintain complete secrecy.

The amount of data, the number of data sources, and the relative lack of human intervention (aka no-touch processes) also contribute to the vulnerability of data to tampering and fraud, and the "time to discovery" can be quite long, necessitating extensive monitoring processes and better controls. Data is also expected to be stored for long periods of time, maybe too long, and can be exposed in compromising ways or inadvertently lost.

The information security threat landscape for manufacturing supply chains, as in oil and gas, is rapidly changing. While traditional DDoS attacks and APTs will continue to represent a major chunk of the threats for manufacturers and their suppliers, security in the industry is expected to have an increasing impact on industrial control systems. Levels of automation continue to rise in factories and in warehouses, and the protection of these systems, which may control devices such as valves, actuators, dosing equipment, or switches on many critical manufacturing assets, will become a key area of investment for these companies. The information security threat landscape for supply chain/manufacturing companies is provided in Table 1.

<table>
<thead>
<tr>
<th>Information Security Threat</th>
<th>Implications for CISOs in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data privacy</td>
<td>Data privacy is at the center of all information security threats. Existing business and transaction models, shifts in the privacy/collaborative balance, conflicts between business and security needs, and legacy data management infrastructure create serious implications for data privacy.</td>
</tr>
<tr>
<td>Data growth and information risk</td>
<td>More digital information, from customer data to sales history to intellectual property, is stored beyond necessary retention time frames. Data is often exchanged between customers and businesses with only limited controls. Data is lost either accidentally or as a result of poorly established risk monitoring systems.</td>
</tr>
</tbody>
</table>
TABLE 1

Information Security in the Supply Chain

<table>
<thead>
<tr>
<th>Information Security Threat</th>
<th>Implications for CISOs in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees' lack of awareness of threats and/or security policies</td>
<td>The security of the company relies on the vigilance and policy-compliant behavior of many individuals, including badged employees, suppliers, and other business partners. A security-aware culture must be fostered among all of these diverse business stakeholders.</td>
</tr>
<tr>
<td>The visibility &quot;paradigm&quot;</td>
<td>Companies face the challenge of providing clarity of business requirements to suppliers while striking a balance between transparency and security.</td>
</tr>
<tr>
<td>Advanced persistent threats (APTs)</td>
<td>Efforts focus on detection capabilities, the implementation of next-generation solutions, and engagement with emergency responders, when required.</td>
</tr>
<tr>
<td>Mobility</td>
<td>Exacerbated by an emphasis on convenience, mobile applications and associated Web services create opportunities for fraud, malware, and unauthorized intelligence collection. BYOD only exacerbates the problem.</td>
</tr>
</tbody>
</table>

Source: IDC Manufacturing Insights, 2014

THE NEW PARADIGM — ENGAGE A SECURITY PARTNER

CISOs must articulate the paradigm shift occurring in security today and the need to change from compliance-based rote actions to requirements for higher-level intelligence. It is critical to have a complete understanding of the threats and available tools and the real dangers associated with working in a vacuum. Emerging and legacy security threats make it imperative for a company to work with a trusted security advisor to assess, design, and implement a holistic security posture. C-suite executives benefit from a security partner's economy of scale, the opportunity to outsource some or all of the enterprise's security needs, and joining forces with a partner to present security challenges to the board.

Nearly all of the security executives IDC interviewed engage at least one security service provider, and most are involved in multiple contracts. There are advantages and disadvantages associated with a single-vendor approach versus a multiple-vendor approach to cybersolution services. While a "one throat to choke" approach is preferred by some executives, many feel that there are few such security services firms that can assist with the full enterprise security need in today's complex environment.

Research respondents consistently suggested that professional services firms are an integral part of their security organizations. Quite often, the service providers manage and monitor a large portion of the security environment. The research respondents caution buyers to vet service providers carefully by looking at expertise, level of education and certification of security staff, and track record. They also caution that it is important to analyze revenue over several years and to investigate whether the service provider is an acquisition target. This concern about acquisition and consolidation is a natural effect of a maturing market that has been disaggregated for a long time.
Some interviewees are cautious about cloud-based services because of data privacy issues and regulatory requirements. Others outsource their entire security environment through a collection of cloud and on-premise solutions with numerous service providers. Federal government agency interviewees are the most cautious. However, pharmaceutical and large supply chain manufacturing respondents also feel they have significant intellectual property and customer data to lose.

Finally, data privacy is a concern across all industries. Executives caution buyers to make sure the service providers they are considering are aware of data sovereignty laws by country and region and that they are capable of working within the requirements of those regions. One pharmaceutical company executive stated that his firm vets service providers over the course of an entire year to study how they train and utilize personnel, determine whether they are an acquisition target, and look at their financials. He stated, "I don't care just about the devices they use."

Some respondents collect and analyze large amounts of threat intelligence data that they collect through their own tools; others subscribe to data feeds and managed services. All stated that it is imperative to actively incorporate data from multiple sources to better prevent zero-day initiatives that are not known signatures. A holistic solution that combines solid knowledge of the constantly evolving threat landscape with the ability to rapidly analyze new and difficult-to-detect threats is critical. A trusted security services partner can help CISOs navigate the twists and turns in the paradigm shift with an eye to containing risk and cost.

CONCLUSION

The challenge of meeting today’s complex security demands is immense. The constantly evolving threat landscape is complicated by budgetary pressures and board-level oversight and the need for intelligence-based analysis of security data sets across the entire enterprise. A holistic response is the only possible course of action. CISOs would be wise to look outside their organizations for expert advice and guidance from a trusted security partner.

The security executives interviewed for this IDC white paper stated clearly that a security services partner should, at a minimum, possess the following:

- An understanding of the business needs by industry
- A comprehensive security services portfolio that ranges from consulting and implementation to managed security services offerings
- Threat intelligence that creates actionable data that feeds into a managed service
- A broad array of security products and partnerships with vendors
- Solid customer testimonials within the buyer's industry
- A strong balance sheet and strong growth trajectory
Essential Guidance

In this white paper, IDC has made the argument that more than ever before the rapidly changing and complex threat landscape across the industries discussed is causing security and risk executives to reevaluate their roles, responsibilities, tools, and skills to protect their businesses from malicious cyberactivity. We proposed the new reality that firms can no longer think simply in terms of the react and defend capabilities delivered by on-premise, signature-based technologies; rather, they must adopt a more holistic approach to security with an emphasis on the ability to predict and prevent. We postulated that this holistic approach requires a clear understanding of threats and their potential impact prior to a security event. We argued that it is through the use of advanced threat detection and analytics that the security organization can prevent infection and minimize risk. We also discussed the future state of enterprise security and the need for reaching beyond mere compliance strategies. Above all, we believe that security and risk executives must be able to articulate these issues at all levels of the enterprise and across all core lines of business. Both security and risk executives are just beginning to recognize that getting to this future state requires greater expertise than is currently available within their organizations and that the current and future security challenges exceed reasonable internal "core competencies" and therefore external security partners may become necessary.

Actions to Consider

The first step in determining whether or not to engage an external security partner is to perform an internal assessment of workload and capabilities. Determine whether your department has the necessary skill set and talent, in addition to budget. Security and risk professionals IDC spoke with agree that the demands of their job, juxtaposed with the advanced threats discussed in this paper, often require them to work with a security partner. However, there are also instances where a company must limit external engagement or manage it very carefully because of regulatory control and data privacy concerns. IDC recommends that companies consider taking the following actions once they have decided on an external engagement:

- Request suggestions from trusted advisors such as clients, companies in the same industry, or third-party experts, and create a short list of security service companies to investigate.
- Examine revenue over several years.
- Some interviewees also recommend investigating whether the firm is an acquisition target and which companies might be courting it. This allows you to analyze the strength of possible acquisition companies.
- Thoroughly vet staff acquisition and the company training model. Look at certifications and continuing education efforts of key security personnel (SOC security analysts, engineers, and others) to remain certified.
- Determine the technology line cards supported and how the partner will integrate into your environment.
- Look for definition of standardized processes in training and security operations handoff.
- Ask about R&D to understand how much revenue is put back into R&D, whether R&D is outsourced, and whether R&D employees are full-time equivalents or contractors. The more R&D is under the purview of the service firm, the greater the chance of consistency in future offerings.
- Investigate any partners of the firm. Much of the security services landscape is a mix of complementary and competitive partnerships as a result of the disaggregated market. Partnerships are not bad in and of themselves; yet not only the primary service firm you seek to engage with but also the partners of that firm.

- Adopt a holistic approach. Respondents to the IDC study agreed that a holistic approach is important. One banking executive summed it up well: "It's not very helpful to only focus on bringing on tools from a tactical perspective and not look at the overall picture."
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world’s leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.988.7900
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

Copyright 2014 IDC Manufacturing Insights. Reproduction without written permission is completely forbidden. External Publication of IDC Manufacturing Insights Information and Data: Any IDC Manufacturing Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Manufacturing Insights Vice President. A draft of the proposed document should accompany any such request. IDC Manufacturing Insights reserves the right to deny approval of external usage for any reason.