WHITE PAPER

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

Sponsored by: Booz Allen Hamilton
Simon Ellis  Shawn P. McCarthy
Eric Newmark  Christina Richmond
Michael Versace  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
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.

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 consequent 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.

©2014 IDC  #246687  2
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

"... At one level [these are] the most trivial type of attacks ... more or less a nuisance. However, we're spending a lot of money protecting the bank." (Global Financial Services Firm)
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.

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)

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)
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, intuiving 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.
Financial Services

Regulatory pressures, budget tightening, and oversight resulting from the economic upheavals of the past decade have been prime motivators for operational risk management investments. These investments remain critical as policymakers and executives stay focused on capital buffers, trade transparency, financial crime, and the impact of cyberthreats on the safety of the financial marketplace. Worldwide, of the $71 billion spent by the financial services industry on technologies and services for risk management, $49 billion is spent on managing operational risks including security and $27.7 billion is spent specifically on information security and fraud.

The increased sophistication of fraud actors, the complexity of the threats, and the size and potential scalability of fraud attacks and losses have placed advanced, predictive threat intelligence solutions and services at the center of security operations.

Risk Mitigation Business Value from Cloud Services

In IDC’s 2013 Vertical Markets Survey of 139 financial institutions, “to gain insight to mitigate risk” was selected as one of the top 3 business values for piloting, selecting, or using public or private cloud services. (IDC Financial Insights)

Among the emerging solutions available to institutions to address these opportunities and challenges are workload-optimized services that support threat analytics workloads on big data, structured and unstructured. For all but a few of the largest institutions and largest targets, these capabilities will be more effectively acquired through services relationships versus those designed, developed, and operated in-house. Firms must carefully examine the trade-offs of outsourcing their security operations against cloud and on-premise integration.
Table 1 represents dynamic threat landscape challenges in the financial services industry and implications that must be carefully considered by CROs and CISOs.

**TABLE 1**

**Information Security in Financial Services**

<table>
<thead>
<tr>
<th>Information Security Threat</th>
<th>Implication for CISOs in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Growth in data and information risk</td>
<td>Growth in data is the fuel for security threats, fraud, and loss. More digital information, from customer data to intellectual property, is stored in insecure areas and beyond necessary retention time frames. Data is often exchanged between consumers and businesses, with few controls across the supply chain. Data is lost accidentally or as a result of poorly established control monitoring systems. IDC Financial Insights estimates that over the past two years, account information from over 450 million customers has been stolen or lost because of porous systems.</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>The speed and scale of cyberattacks continue to accelerate — in most cases, faster than enterprise defense systems. Well-funded professional crimeware companies are a growing threat. Other “actors” (espionage groups, terrorists, hackers, and rogue insiders) are often subsidized and coordinated by well-funded, innovative global organizations. Intellectual property and control disruption are primary targets of attack.</td>
</tr>
<tr>
<td>“React and remediate” defenses</td>
<td>Simple compliance strategies are failing at a spectacular rate. The costs associated with existing defensive measures and built into security operations centers are scaling up at an unsustainable rate. A predictive perimeter of intelligence has become a net add and a table stakes requirement for operations centers and all access points.</td>
</tr>
<tr>
<td>Data privacy</td>
<td>Data privacy is at the center of the threat environment. Shifts in the privacy versus convenience exchange rate will continue to occur. (IDC Retail Insights found that when consumers are given the choice between privacy and convenience, there’s a close-to-even split.)</td>
</tr>
<tr>
<td>Cloud</td>
<td>“Gaining insight to mitigate risks” is one of the top 3 reasons financial institutions move to cloud services, both public and private cloud arrangements.</td>
</tr>
<tr>
<td>Demand for security talent</td>
<td>The 3rd Platform of IT (cloud, big data and analytics, mobile, and social) will change the demands on 95% of all IT skills, including security, over the next three to five years. This ultimately changes the balance between in-house skills and skills acquired through service providers.</td>
</tr>
</tbody>
</table>

Source: IDC Financial Insights, 2014
**Government**

Government IT security directors often find themselves in a unique situation. Their legacy systems can range from older IT mainframe systems to very recent cloud-based and mobile applications. Security solutions need to extend across the full range of old and new, and engineers who have experience in systems integration often serve as the talent base for enterprisewide IT security.

Many government agencies have seen an increase in APTs – some of which can lurk on networks for weeks or months before they are detected. Thus, advanced network monitoring tools and consistency checks are proving useful for helping protect government networks. Another area that is highly important to government IT managers is access control management. This can include machine-to-machine access or person-to-machine access. Accurate access control management, combined with consistent enforcement, can greatly reduce both external and insider threats. In many cases, access control must also be integrated with employee ID cards via requirements that are outlined in initiatives such as the Homeland Security Presidential Directive 12 (HSPD-12).

Configuration management also is a key security issue for many government agencies. Some CISOs interviewed discussed tools they have in place to remotely monitor and manage most configuration settings. But it is apparent that configuration monitoring at some agencies is focused more on detection. Remote management (changing or resetting configuration) is more rare. In-person visits to equipment to handle the configuration work is still common. Another role played by government is that of an advisor for other industries, such as monitoring threats to industrial control systems or financial systems and advising industries on mitigation techniques. Sometimes this requires very specific tools for detection and very specific approaches for mitigation. Highly skilled contractors with narrowly defined mitigation technologies are sometimes brought in to address specific infrastructure threats.

Some CISOs noted a preference for having security personnel located in-house, even if the employees are contractors. Also, depending on the sensitivity of data, some agencies are very cautious about exploring security services (network monitoring and management, configuration management, threat scanning) that are managed externally. Likewise, they are wary of potential security concerns related to hosting sensitive data out in the cloud.

Many federal agencies have appointed chief security officers who help detect and coordinate responses to security issues. However, overall security still falls on the shoulders of the CIOs for integrating security for IT and business functions, as well as assuming the risk when external services are selected. CIOs need to confirm that such choices are acceptable to the organization and compliant with both internal and governmentwide security policies.

Most government agencies have specific requirements related to compliance with Federal Information Processing Standards (FIPS) or security rules related to the Federal Information Security Management Act (FISMA). Many agencies now are also requiring continuous monitoring of select IT resources to ensure that problems or threats are quickly detected. The information security threat landscape for government is provided in Table 2.
## TABLE 2

<table>
<thead>
<tr>
<th>Information Security Threat</th>
<th>Implication for CISOs in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>The greatest ongoing threat is from foreign governments or foreign entities that have political or philosophical agendas. Threats may range from military-related probing to antigovernment system vandalism. Sometimes they are done by people whose government doctrines actually encourage such actions, which makes it difficult to seek help from the place where an attack is originating.</td>
<td>Agencies need to integrate advanced detection or prevention systems. These solutions need routine upgrades, and the solutions continue to grow in sophistication. Many agencies are decreasing the number of Internet connections they have in order to better monitor and control access via designated gateways.</td>
</tr>
<tr>
<td>Many organizations are experiencing hundreds of attacks per day and also discovering embedded advanced persistent threats (APTs).</td>
<td>One key step is to educate top-level managers so that they understand that security investments will be an ongoing &quot;cost of doing business.&quot; Monitoring tools are one of the key investments for detecting these types of security threats.</td>
</tr>
<tr>
<td>Industry infrastructure protection</td>
<td>Agencies need to work closely with industry to monitor threats and keep businesses informed when threats grow and when tools are available to counter the threats.</td>
</tr>
<tr>
<td>Distributed denial-of-service (DDoS) attacks</td>
<td>DDoS attacks are common against government agencies. Solutions include detecting and redirecting malicious packets and temporarily reassigning domain names and Internet Protocol addresses to keep improper Internet Protocol traffic at bay.</td>
</tr>
<tr>
<td>Employees may try to use Internet protocols that are not inherently safe (such as FTP or peer-to-peer file sharing).</td>
<td>Unsecure and unapproved connections can become gateways for possible viruses or malware. Some agencies block specific protocols or ports by default, right at their firewalls. Also, when employees want to communicate with an external service provider, some agencies require those requests to be vetted, sometimes via a change control committee that will review such requests.</td>
</tr>
<tr>
<td>Authentication control</td>
<td>Today, many agencies rely on Windows Active Directory infrastructure, or some other protocol, for authentication. Some agencies are investigating hosted authentication management solutions, but their use is not yet widespread. Compliance with mandatory access control protocols is key.</td>
</tr>
</tbody>
</table>

Source: IDC Government Insights, 2014

### Oil and Gas

The issue of data security is not a new challenge for most oil and gas companies, but the rapid development of data-intensive processes in the industry, such as the digital oil field or integrated operations, has led a large majority of companies to consider the protection of commercially sensitive data and corporate IT assets as a top priority in the recent years. Critical information for any upstream
company includes exploration data (such as seismic, reservoir mapping, or drilling data), production data (production rates or reserves data), and financial/contractual data (hydrocarbon accounting and production sharing agreement data). Additionally, oil and gas firms are facing more complex and harsh technical and environmental challenges – in remote locations such as Africa – which increase the difficulty in protecting against cyberthreats.

The question of cybersecurity has gained even more momentum among oil and gas decision makers in the past three years, following a trend of major attacks intending to disrupt specifically the operations of various industry leaders across the globe. The so-called Shamoon incidents have, for instance, drawn a lot of public attention to the potential degree of disruption caused by highly sophisticated attacks for major oil and gas companies. These incidents are not isolated occurrences: Other cyberattacks, such as Operation Night Dragon, Project Tarmaggedon, Poison Ivy, or Operation Save the Arctic, have targeted, and in some cases have successfully affected, the operations and businesses of some of the largest companies in the oil and gas and chemical industries.

The information security threat landscape is rapidly changing: Classic DDoS attacks and APTs will continue to represent a major chunk of the threats for oil and gas companies, but the question of security in the industry is expected to go beyond "traditional" IT and to start impacting industrial control systems. The protection of these systems, which control electromechanical devices such as valves or switches on many critical oil and gas assets, will become a key area of investment for most oil and gas companies in the near future as end users become more and more aware of the vulnerability of legacy control systems, the impact of IT/OT convergence in terms of network protection, and the financial consequences of such attacks on their operations. The information security threat landscape for oil and gas companies is provided in Table 3.

**TABLE 3**

<table>
<thead>
<tr>
<th>Information Security Threat</th>
<th>Implications for CISOs in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration of rogue employees</td>
<td>There is a need to focus on identity and access rights policies and the development of advanced identity management solutions.</td>
</tr>
<tr>
<td>Employees' lack of awareness of threats and/or security policies</td>
<td>It is important to foster a security-aware culture among employees.</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>Industrial control system threat</td>
<td>Endpoint vulnerabilities and the implementation of state-of-the-art protection systems and business continuity plans need to be reviewed.</td>
</tr>
</tbody>
</table>

Source: IDC Energy Insights, 2014
Supply Chain/Manufacturing

The increasingly distributed nature of the manufacturing supply chain is putting it at 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 4.

<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>
<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>
</tbody>
</table>
TABLE 4

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>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

Pharmaceuticals/Life Sciences

The life sciences are working through a challenging period of industry change, accosted by regulatory changes and shifting market dynamics from U.S. healthcare reform, all in light of significant pressure to continue reducing costs. Companies have been working to shift more focus to specialized therapeutic niches, orphan drugs, and even OTC drug opportunities to help diversify product portfolios and insulate themselves from further healthcare legislative turmoil. However, while life sciences companies have been dealing with patent protection and cost-related challenges for over a decade, a newer challenge that has emerged in the past few years is cybersecurity.

With broad migration of most life sciences software now moving to the cloud as a primary platform, the industry has increased its exposure to the effects of DDoS and related types of attacks that could cause significant downtime and affect the productivity of everything from sales activity and manufacturing efficiency to the speed and efficacy of clinical trials. Even more critical in nature are the effects of APTs, which are quickly becoming a focal point for life sciences IT and security personnel because of the damage they can cause. Roughly $10 billion goes into the research and development (R&D) behind each new drug. Security surrounding that information is critical because stolen IP could cost a company billions of dollars and dramatically affect the future viability and direction of the company. We’ve seen examples of this in the medical device industry, where IP stolen from a U.S. company regarding a device under development for over five years was sent to China, thus enabling a Chinese competitor to release the same device in less than a year.

One aspect of the life sciences industry evolution that is of significant concern from a security standpoint is the vast adoption of mobile devices, with particular focus on BYOD policies expanding across many companies. Ensuring that proper security is in place across all devices, and that all access points into each company’s network are secure, is becoming an increasingly difficult task. Investment in remote device management is also gaining steam because employees in the field can easily misplace a laptop or their phone or tablet may be stolen. The ability to secure and remotely
erase all data on these devices is vital because both customer data and product-related IP often exist on the devices and can easily end up in the wrong hands. The information security threat landscape for pharmaceuticals companies is provided in Table 5.

### TABLE 5

<table>
<thead>
<tr>
<th>Information Security Threat</th>
<th>Implications for CISOs in the Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility and BYOD</td>
<td>There is a need to balance convenience with security. The broadening set of devices with access to corporate networks exacerbates opportunities for fraud, malware, and unauthorized intelligence collection. BYOD only exacerbates the problem.</td>
</tr>
<tr>
<td>Employees’ lack of awareness of threats and/or security policies</td>
<td>It is important to foster a security-aware culture among employees, particularly those using mobile devices loaded with sensitive customer data or product-related IP.</td>
</tr>
<tr>
<td>Advanced persistent threats (APTs)</td>
<td>There is a strong focus on detection capabilities, implementation of advanced security solutions, and the need to establish relationships with third-party security partners with deep expertise based on real-world security breach experience.</td>
</tr>
<tr>
<td>Cloud adoption</td>
<td>The broad movement of software to the cloud across the enterprise creates new security challenges and potential downtime risk from DDoS attacks.</td>
</tr>
<tr>
<td>Demand for security talent</td>
<td>The 3rd Platform of IT (cloud, big data and analytics, mobile, social) will change the demands on 95% of all IT skills, including security, over the next three to five years. This ultimately changes the balance between in-house skills and skills acquired through service providers.</td>
</tr>
</tbody>
</table>

Source: IDC Health 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; vet 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
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2014 IDC. Reproduction without written permission is completely forbidden.