White Paper

Cybersecurity Readiness: How "At Risk" Is Your Organization?

Sponsored by: AT&T

Christina Richmond
May 2017

EXECUTIVE SUMMARY

IT security is a subject that is top of mind for senior executives around the world. But despite the recent spate of high-cost, high-profile attacks such as those experienced by Sony and Target, security is something that many C-level executives and board of directors fail to provide appropriate attention to, believing they can delegate to their IT organizations, or that they can "set it and forget it."

"[High-profile] breaches make security front of mind for the business for a very short period of time. The board of directors and CEOs ask questions about it. Then day-to-day business takes over, and it goes way." — SVP of Marketing, Large Consumer Products Firm

IDC calls this the overconfidence trap, and getting their boards and C-suite not to fall into the overconfidence trap is one of the key challenges facing CIOs and CISOs today. The question is no longer if or when you will be breached, but rather how often and how severe the breaches will be. But even more important is whether you will be adequately prepared to:

- Detect attacks
- Quickly recognize a breach
- Effectively remediate the attack
- Accurately assess the damage

"[A] 'secure enough' concept just doesn't exist. It's not a finite process. It's constantly changing." — Chief Information Security Officer, Financial Services Firm

IDC conducted a study of C-level executives responsible for IT security in organizations around the world to better understand the enterprise security landscape and readiness of organizations today. This study identified four levels of IT security readiness. These levels from highest to lowest readiness are:

- **Progressive.** This is the highest level of security readiness. C-level executives at progressive companies play very close attention to security, with a strong role in setting, managing, and reviewing their security stance. These companies understand that they are targets of breaches. Because these companies are regularly attacked and sometimes breached, they actively use advanced security technologies as proactive steps to sharply reduce (or eliminate) the value of compromised data to hackers. They perform near-constant security reviews and use third-party service providers (SPs) to take advantage of the service providers' substantial expertise to supplement the bandwidth of their internal security teams.

- **Proactive.** Proactive companies have above-average levels of security readiness, although they are not as high as progressives. Proactive companies realize the importance of IT security and have put in place basic steps to avoid breaches, although they are less likely to use technologies such as tokenization to minimize the value of data that hackers could compromise. C-level executives pay close attention to security and realize they are at risk of being breached. Proactives tend to perform monthly reviews of their security position and regularly perform risk assessments. Their primary motivation to use third parties is to supplement the bandwidth of their internal security team.
- **Reactive.** Reactive companies have below-average levels of security readiness. C-level executives pay moderate attention to security while delegating security expertise and day-to-day management to IT. Reactive companies realize they are at risk of breach and are aware of many breaches. They react to breaches on a case-by-case basis. They perform quarterly reviews of their security stance and third-party risk assessments. They look to third parties to supplement their internal expertise.
- **Passive.** Passive companies are the least security ready. At passive companies, C-level executives take a hands-off stance to security with all knowledge and responsibility incumbent upon IT. They would prefer that the IT security issue would simply go away, tending to be unaware of most breaches and reactive in response to breaches they do detect. Reviews of the security posture and third-party risk assessments of passive companies are infrequent, occurring twice a year or less frequently. And they are much less likely to look to third parties for help.

IDC found that the companies with the highest levels of IT security readiness also had the greatest levels of business success across nearly every dimension studied including revenue growth, profitability, and employee productivity. In other words, being security ready is good for business. Notably, IDC did **not** find that security readiness led to fewer breaches; in fact, the highest-readiness companies were more likely to have reported encountering more breaches, and those breaches were more severe.

IDC believes that there is a bit of a chicken/egg effect at work in these findings: higher-readiness companies may not have that many more actual security breaches; they are just more aware of the ones they have. In addition, IDC believes that these companies are **forced** to have higher levels of readiness **because** they are breached a lot. In other words, they report more attacks and breaches because they are actively looking at them. Many of these companies (including banks, insurance companies, and retailers) are tightly regulated, so breaches are painful and require careful assessment before notification to limit damages. These firms have no choice but to implement state-of-the-art security practices. In a strange twist, IDC believes that some frequently breached companies are doing security better, not worse.

Finally, this study characterized the habits, practices, and investments of higher security-ready companies. The highest-readiness companies are characterized by:

- Senior level of management playing greater roles in setting, managing, and reviewing IT security policy and practices
- Highest year-over-year growth in security budgets and the greatest use of advanced security solutions and technologies
- Greater frequency in performing security reviews and third-party risk assessments
- Greater overall reliance on third parties and greater spend on third-party support

It's clear that companies across all industries and geographies are looking to improve security readiness. Not only does readiness improve compliance and reduce risk to the business, but this study showed that greater readiness is also linked to broader measures of business success. Every company should assess its security readiness, and the Readiness Index Tool that IDC developed as part of this study is a good starting point.

One critical element of improving readiness is bridging the gap between IT and the board of directors and C-suite. Too many IT organizations talk about security in terms of technologies, programs, and threat levels. Instead the IT organizations need to learn to:

- Communicate how improved security stance fits with overall corporate strategy
- Focus on investment that leads to better business results
- Look closely at security spend, and see to it that they are investing in fundamental technologies such as vulnerability management, data security, and cloud solutions
- Bolster their in-house team with third-party SPs because it is increasingly difficult to hire and retain knowledgeable staff to do it all themselves

About This Study

This IDC study is based on a global survey of 802 IT executives and line-of-business (LOB) executives. The respondents came from organizations having 1,000+ employees across a broad range of industries. The survey was supplemented with a focus group of CIOs and CISOs from enterprises with 1,000+ employees. For a more detailed description of the study methodology, see the Appendix.

The Overconfidence Trap: Organizations Are Not as Ready as They Believe

Security is a moving target, and the concept of achieving an acceptable level of security is not a static state. New threats are emerging, bad actors are constantly looking for security vulnerabilities, and the work of the security team is never "done." And no company is truly safe or can rest assured that it will not be the target of an attack. For most companies, it's not a question of whether they will be attacked or even when, but how often and how severe the attacks will be. To quote the late Andrew Grove, former CEO of Intel, "Only the paranoid survive."

"I've seen situations where security budgets were based on compliance goals. As soon as they got compliance, the money stopped, but they were only 10% of the way to the level they needed. And that is such a trap." — Chief Information Security Officer, Financial Services Firm

Further, simply demonstrating compliance with industry and security standards is also not enough. In fact, compliance can be a double-edge sword: C-level executives often think that because their organizations have compliant processes, staff, and systems, they have "checked the security box." The reality is that compliance is not a guarantee of security, and a great many breaches occur within compliant organizations. Helping their organizations avoid this false sense of security is a mission for most CIOs and CISOs in today's enterprise.

IDC's Four Levels of Security Readiness

To understand different security stances and their impact on business outcomes, this study categorized the level of security readiness at large and midsized companies across a variety of security policies, practices, and uses of technologies. Companies were measured and ranked by behaviors that were most closely linked to positive business outcomes.

Only 16% of the companies in our study displayed the highest level of security readiness. We call these companies "progressive." These companies excelled across all the security aspects measured and reported the strongest business results.

Table 1 provides a summary of the four levels as well as their key characteristics.

"It boils down to data classification. You protect your really valuable stuff in the safe and then the other stuff you put in your closet, out in the living room, or even in the front yard." — CISO, Healthcare Provider

TABLE 1

Security-Readiness Category Profiles

Passive	Reactive	Proactive	Progressive
C-level management is hands-off and delegates nearly all security responsibility to IT	C-level executives pay moderate attention; rely on IT for expertise and day-to-day management	C-level executives pay close attention to security but partner with IT for day-to-day management	Senior C-level executives play a strong role in setting, managing, and regularly reviewing security stance
Unaware of most breaches; react slowly and chaotically to breaches	Realize breach has occurred but respond slowly on case-by-case basis	See attacks, realize they are being breached, and proactively work to avoid breaches	Know they are regularly breached and proactively work to make breaches unappealing to hackers (mitigate the value of the data hackers can access)
Infrequently review security policies and processes and perform few third-party risk assessments (two times per year or less)	Review security stance and perform third-party risk assessments quarterly	Review security stance and perform third-party risk assessments monthly	Perform ongoing security reviews and third-party risk assessments
Rarely look to third parties for help	Use third parties to supplement limited internal resources and expertise	Focus internal resources on critical tasks while using third parties to supplement internal personnel bandwidth	Focus internal resources on critical tasks while using third parties to augment internal personnel expertise
Representative industries include education, mining/agriculture, and life sciences	Representative industries include transportation and energy/utilities	Representative industries include retail, healthcare, and media	Representative industries include banking and insurance

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

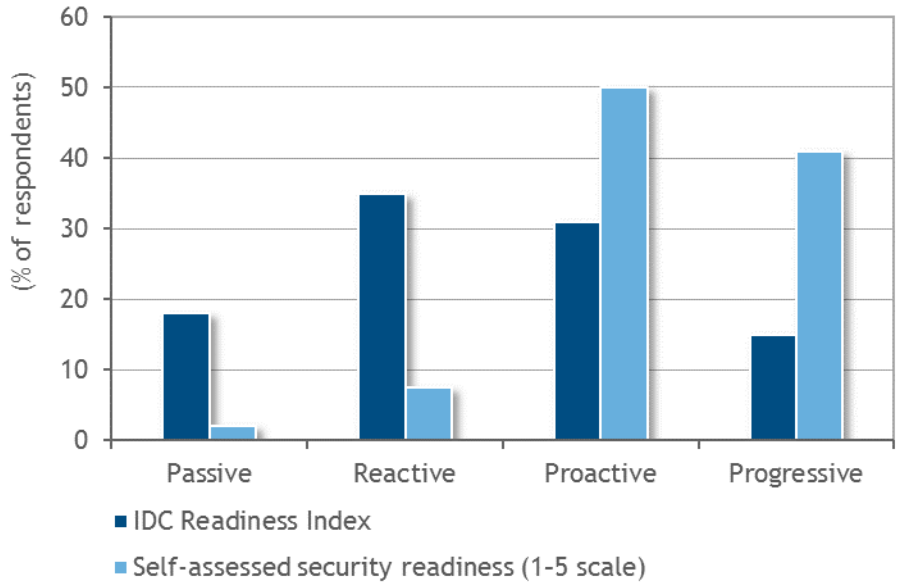
While there were discernable differences by industry, as noted in Table 1, it's notable that there were no meaningful differences by organizational size. In other words, organizational size had little to no predictive effect on a company's security stance.

Security Readiness: Perception Outstrips Reality

Most companies believe they are far more ready than they actually are. When asked about their level of readiness, 41% of companies called themselves extremely secure (i.e., they gave themselves a 5 on a scale of 1–5), and 50% of companies rated themselves as very secure. This means that only 9% of companies believe they are not very secure. In contrast, IDC's analysis shows that only 47% of organizations fall into one of the top 2 security categories (16% of organizations are progressive, and 31% of organizations are proactive), while the other 53% of organizations are at risk (see Figure 1).

FIGURE 1

Readiness Perception Far Outstrips the Reality



n = 802

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

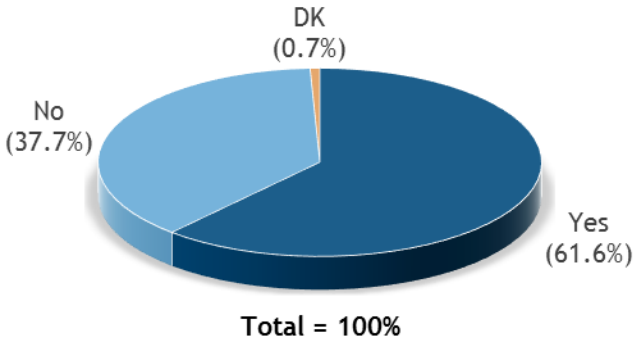
This discrepancy between perception (self-assesses security readiness) and reality (IDC Readiness Index) is a huge challenge for enterprises. Having a false sense of readiness can be very dangerous because it can leave organizations blind to their own vulnerabilities, or even the need to consider those vulnerabilities. Instead, organizations should look to independent assessments of their readiness to help them understand how prepared they are for the eventual, inevitable attacks on their systems and data.

Security Breaches Are Prevalent

Underlining the prevalence of security breaches, most of the companies in our study reported having experienced breaches. Fully, 61.6% of respondents said their organizations were breached in the past 12 months (see Figure 2).

FIGURE 2

Organizations Experiencing IT Security Breaches



n = 802

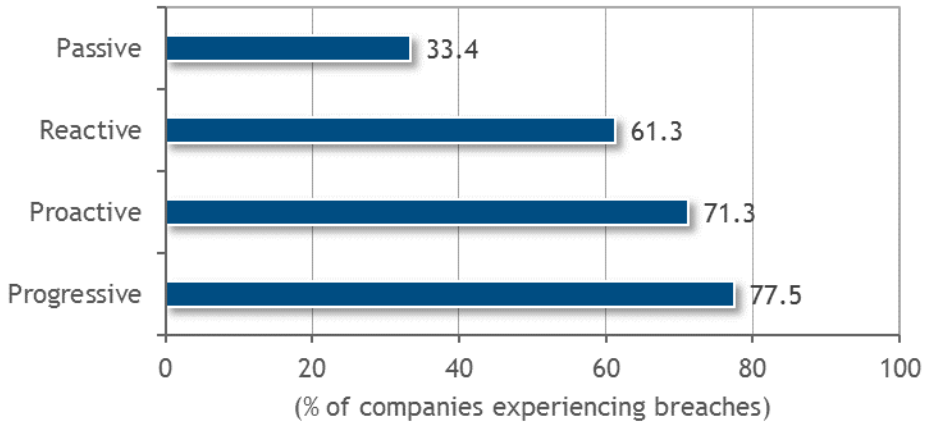
Note: Respondents were asked if they experienced one or more IT security breaches over past 12 months.

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Interestingly, higher-readiness companies were more likely to have had a breach over the past 12 months. Over 77% of progressive companies and 71% of proactive companies experienced breaches compared with only 33.4% of passive companies (see Figure 3).

FIGURE 3

Breach Incidence by Readiness Level



n = 802

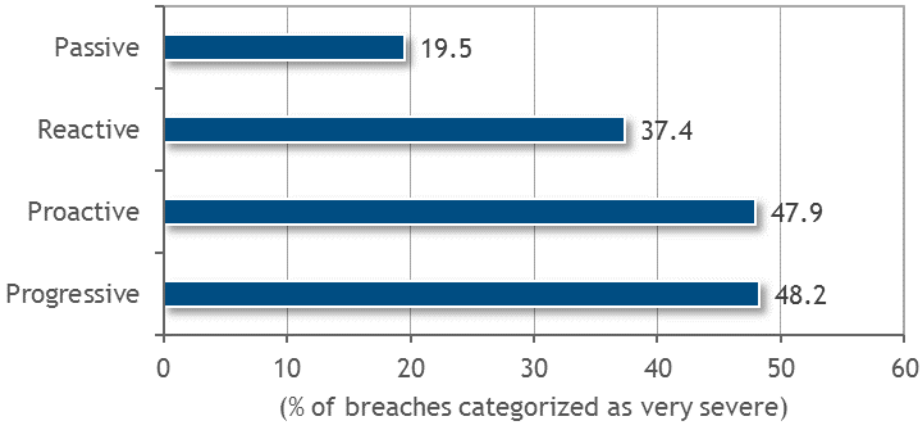
Base = companies that said they have experienced one or more IT security breaches over past 12 months

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Further, the greater the level of security readiness, the more severe the impact of breaches. Progressive and proactive companies classified around 48% of breaches as "very severe" compared with reactive companies that classified 37.4% of breaches and passive companies that classified only 19.5% of breaches (see Figure 4).

FIGURE 4

Breaches Categorized as "Very Severe"



n = 802

Notes:

Percentage of organizations that classified their most severe breach as having "very severe" business impact.

Data represents top 2 box rating on a severity scale of 1-5, where 1 = not severe and 5 = very severe.

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

While these findings may initially seem counterintuitive, IDC believes there are several factors at work, including a measurement effect. Low-readiness companies are less likely to be aware of the breaches they do have because they have fewer best practices in place to detect and address them. So there is likely undercounting of breaches among passive companies.

High-readiness companies are more likely to be attacked. These companies have higher readiness because they need to be; they are more likely to detect and quickly react to breaches. So the higher levels of breach incidence among progressive and proactive companies are not a reflection of a failure in their security stance, rather their security stance is a reflection of the incidence of breaches they receive. The higher levels of breaches among progressive and proactive companies are not necessarily indicative of holes in their security stance; instead, these companies likely have better security practices because they need to.

The Link Between Security Readiness and Business Outcomes

Security-Ready Organizations Enjoy Better Business Results

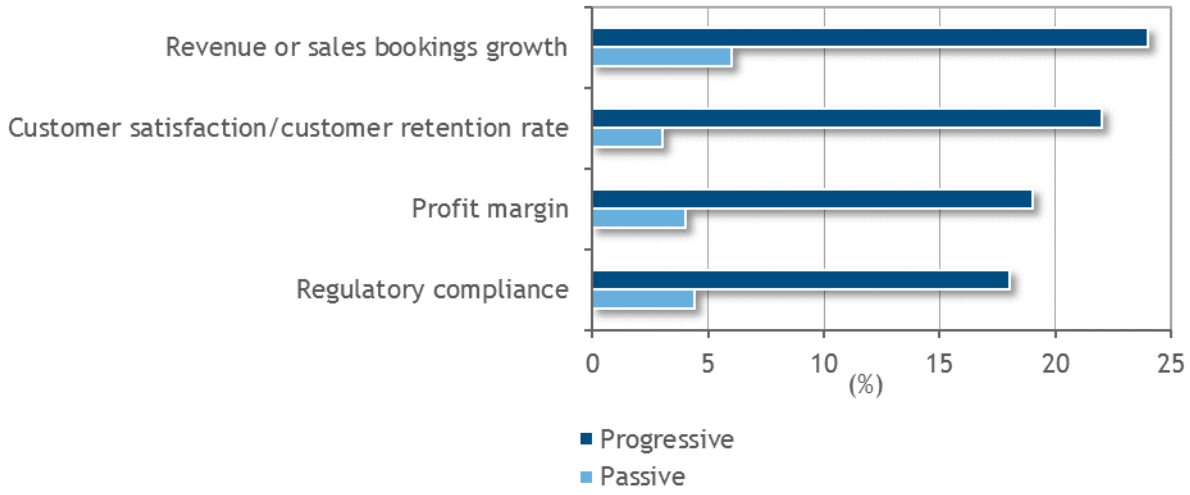
The study showed that progressive and proactive organizations exhibit better business outcomes.

The difference can be easily seen when comparing the most-ready organizations versus least-ready organizations. Progressive companies experienced dramatically superior outcomes across every business key performance indicator (KPI) in the study compared with passive companies. For example, the sales growth over the past three years for progressive companies was 24% compared with 6% for passive organizations; the customer satisfaction for progressive companies increased 22% compared with 2% for passive companies, and the profit margin for progressive companies grew by 20% compared with 3% for passive companies (see Figure 5).

"Selling security for security sake is hard. But selling security because it will let you do something you couldn't otherwise do is very easy, especially if it can generate sales." — Chief Information Security Officer, Financial Services Firm

FIGURE 5

Past Three-Year KPI Improvements



n = 125 for progressive companies, n = 142 for passive companies

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Initially, the link between security readiness and business outcomes may seem a stretch, but this is a topic IDC explored in a focus group conducted for this research. CIOs and CISOs in the focus group mentioned a number of ways that improved security can also lead to greater efficiencies and improved user experience. These ways included single sign-on, encryption, data tokenization, mobile device management, and guest VLAN access. Furthermore, the reader should note that this linkage is based on correlation, which may or may not imply causality. Organizations with more strategic, sophisticated approaches to IT may be more successful in general, as well as be more security ready.

But regardless of the nature of the linkage, IDC notes that more security-ready companies do achieve better business results, and IDC strongly believes it is to every organization's benefit to become as security ready as it can.

What It Takes to Become IT Security Ready

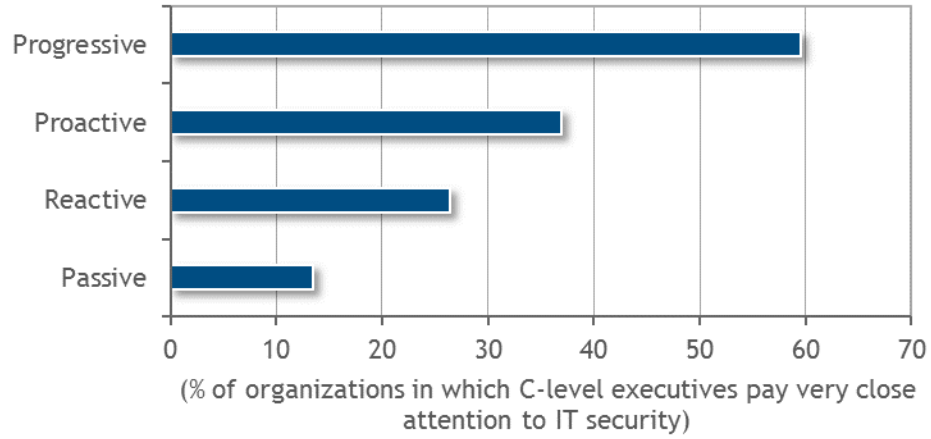
Security Readiness Starts at the Top

Security readiness is something that permeates the organization, starting with the board of directors and C-level executives. IT cannot be expected to "go it alone." Those individuals in the line of business need to be engaged not only because employees must adhere to policies and best practices but also because lines of business need to be engaged in understanding the key assets that require protection and the most appropriate means of protecting them.

Our study reinforced the importance of providing C-level attention to security. Of all, 60% of progressive organizations say their C-level executives pay "very close" attention to security, with daily status updates and monitoring on a hands-on level. In contrast, only 14% of passive companies' C-level executives pay very close attention to security and instead are much more likely to leave day-to-day security management to IT (see Figure 6).

FIGURE 6

Paying Very Close Attention to Enterprise IT Security



n = 802

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

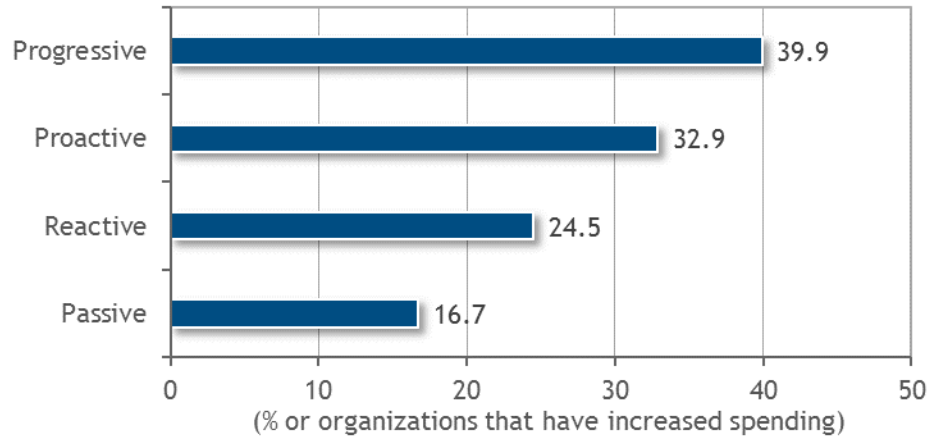
Security-Ready Organizations Are Increasing Their Security Investment

Being security ready requires appropriate investment in people, processes, and technologies. The most advanced organizations in our study have the highest levels of investment increase from year to year.

Progressive organizations increased their security spend by 40% compared with passive organizations, which increased security spend by a comparatively moderate 17%, from 2015 to 2016 (see Figure 7).

FIGURE 7

Increase in Security Spend, 2015–2016



n = 802

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Note that survey respondents told us that on average across all categories of business the security spend is currently around 17% of their IT budgets, a figure that is in line with the security level that IDC sees in other security studies.

Security-Ready Organizations Perform More Frequent Risk Assessments and Reviews

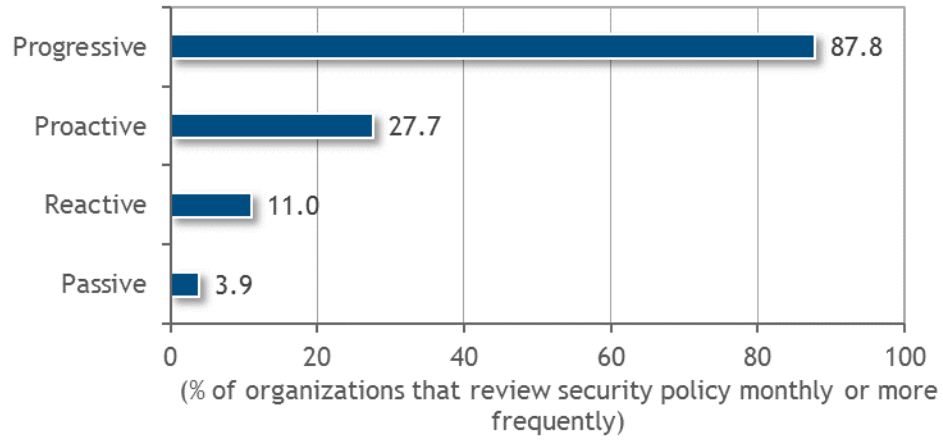
With nearly every aspect of today's enterprise using IT systems, the goal of protecting each of those systems is a difficult task. One of the most important aspects is performing assessments of security needs and risks and identifying the corporate assets most in need of protection. Businesses should understand the costs associated with system failures and compromised data, including their connection to intangibles like brand reputation and customer retention. These risks equate to costly long-term risk that necessitates senior management oversight.

"I don't think a lot of companies actually go through the whole exercise of doing risk assessments, but in truth, that's what you are supposed to be doing: identifying the assets you want to protect." — Chief Security Officer, Financial Services Firm

Security reviews and assessments cannot be done once or even every now and again. With systems, data, risks, and threats changing on an ongoing basis, organizations need to be constantly assessing and reassessing their security policies. This point is borne out by the study: the most security-ready organizations perform risk assessments and vulnerability scans almost continuously compared with less security-ready companies that perform risk assessments and vulnerability scans quarterly or annually (see Figure 8).

FIGURE 8

Conducting End-to-End Review of IT Security Policies Monthly or More Frequently



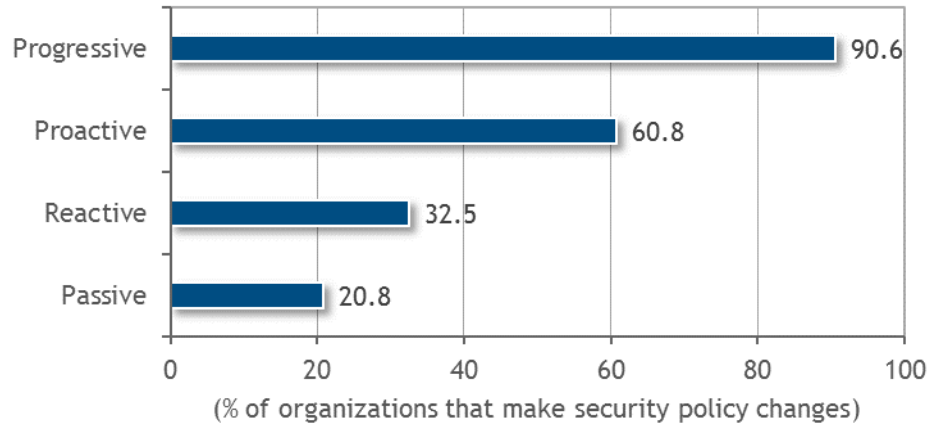
n = 802

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Not only are progressive organizations performing more frequent reviews, but they are also much more likely to make substantive changes as a result of those reviews. As shown in Figure 9, progressive companies take direct action based on these scans. Reactive and passive companies may choose to take no action or defer remediation on vulnerabilities because they are not relevant to compliance or they don't have the staff to address the volume of vulnerabilities. This failure will open up these companies' systems and applications to attacks and breaches.

FIGURE 9

Making Substantive Changes in IT Security Policy Based on Each Security Review



n = 802

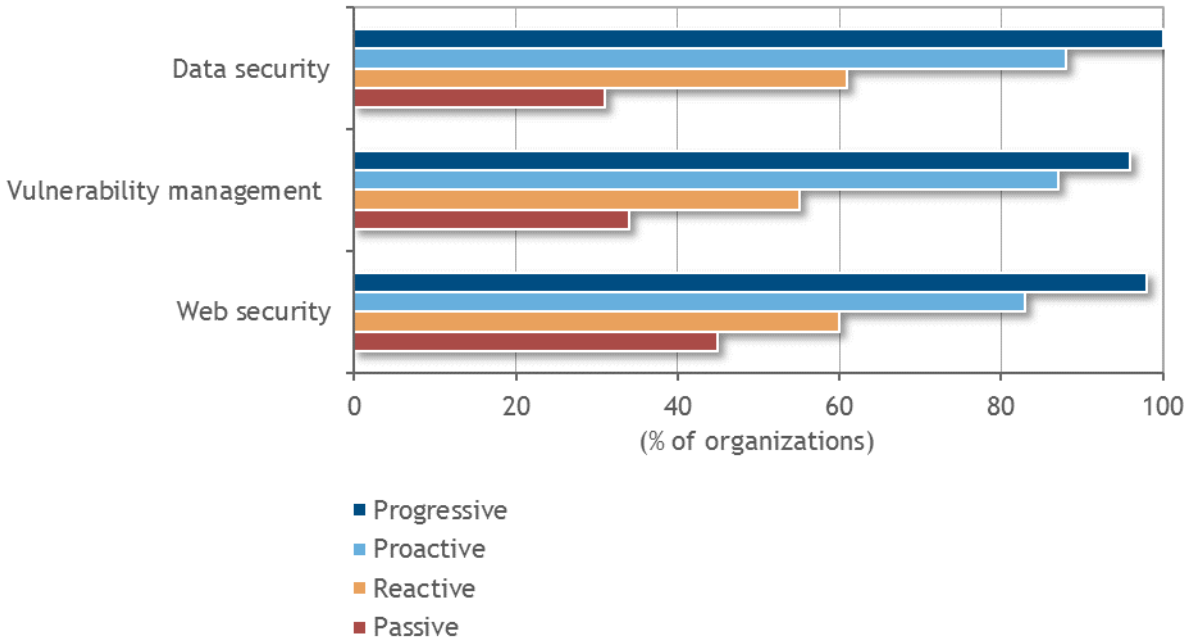
Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Advanced Technologies and Solutions

Consistent with the finding that security-ready companies are investing more in security overall, this study found that they are more likely to be investing in specific technologies. The specific technologies include data security, vulnerability management, and web security (see Figure 10).

FIGURE 10

Making Significant Investments in Technology Solutions Over the Next 12 Months



n = 802

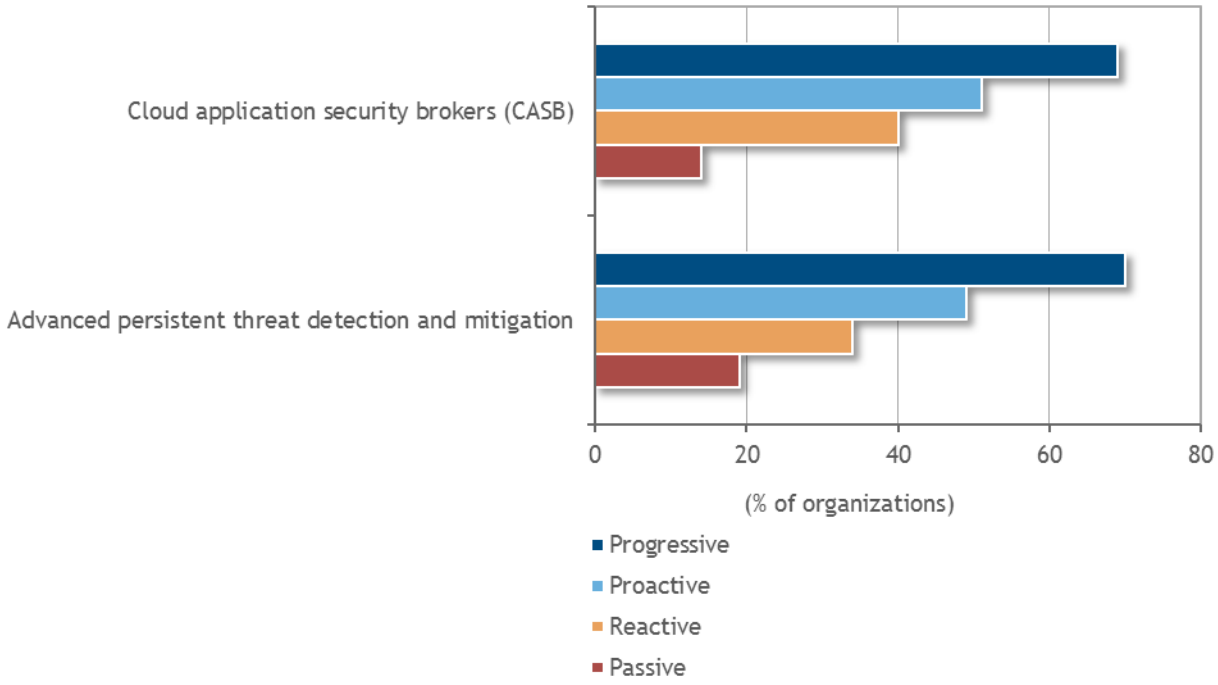
Note: Data represents top 2 box scores on a scale of 1-5, where 1 = no investment and 5 = significant investment.

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Perhaps even more tellingly, highly security-ready companies are more likely to be using advanced security technologies such as advanced persistent threat detection and mitigation as well as cloud applications security brokers (CASB) to more securely manage other SaaS applications (see Figure 11).

FIGURE 11

Current Use of Technology



n = 802

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

Use of Third Parties

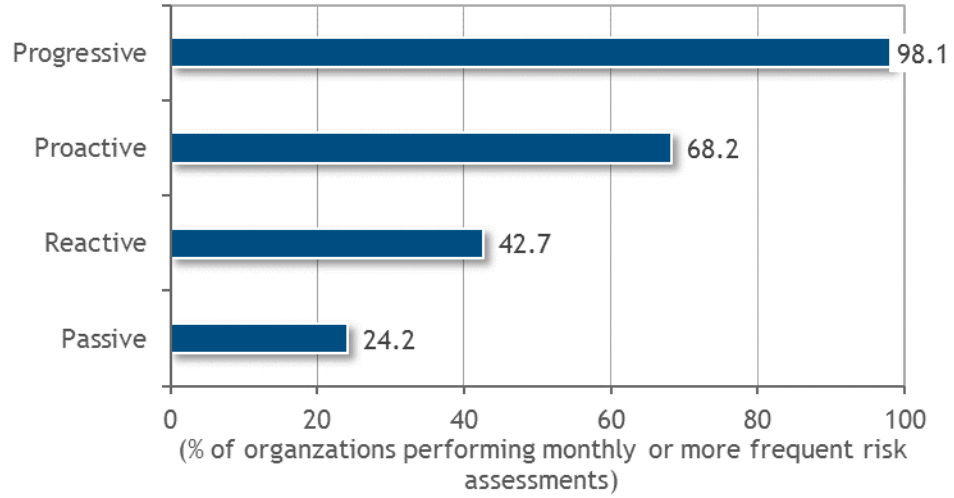
Another key dimension separating levels of security readiness is stance toward the use of third parties. The least-ready companies tend to focus more on the use of internal staff resources and do not utilize the supplemental bandwidth and security expertise that third-party providers can bring to the table. In contrast, proactive companies focus their in-house talent on the most critical tasks while outsourcing other tasks to third parties to supplement internal bandwidth, while progressive companies take that a step further and outsource tasks to third parties to take advantage of the expertise those providers bring.

One example of greater use of third parties comes in the greater likelihood for more security-ready companies to perform frequent third-party risk assessments (see Figure 12).

"It is really hard to get skilled security people that can understand business as well. And if you can get them, the price for them is getting to be outrageous." — Chief Information Security Officer, Financial Services Firm

FIGURE 12

Performing Independent/Third-Party Risk Assessments or Penetration Monthly or More Frequently



n = 802

Source: IDC's *Enterprise IT Security Readiness Index Survey,* January 2016

The higher-readiness companies also spend more on third-party providers to deal with breaches: progressive companies are more than three times as likely to have executed new third-party service provider contracts as a result of security breaches and are twice as likely to have expanded existing third-party service provider contracts to deal with breaches.

"We are trying to hire a company to run our existing security infrastructure. We have a number of top-tier tools, and I've got more tools than I have people to run them." — Chief Information Security Officer, Financial Services Firm

ESSENTIAL GUIDANCE

Security readiness is critical to business' success in today's data-driven world, yet this study found that only 16% of companies were found to be progressive, the group with the highest level of security readiness. With a highly secure IT infrastructure and strong security best practices, progressive companies are in a better position to survive the inevitable breaches facing enterprises today and, not coincidentally, they achieve superior business outcomes.

But what about everyone else? Are 84% of companies doomed to suffer from being less security ready? The answer is no. Organizations at all levels can improve their security readiness, and by implication, they realize greater business benefits. Key steps in the journey include:

- **Bridge the gap between IT and the board/C-suite.** Many CIOs and CISOs continue to think of the world in terms of IT and security architectures, threat detection, and avoidance and mitigation. To many boards and C-level executives, including CEOs, CFOs, and COOs, this is a foreign language, and such arguments fall on deaf ears. CIOs and CISOs need to get out of

the habit of talking "geek speak" and instead become comfortable discussing strategic threats and opportunities to the business and building and presenting business cases to the CFOs. These business cases should be couched in terms like *return on investment, improved compliance, improved customer experience,* and *improved employee productivity.*

- **Make your board and CEO read this white paper.** As this study shows, there is a statistical link between having a superior security stance and improved business outcomes. Security is of great importance to the board and CEO, and the ability to show the linkage with business outcomes could be a strong incentive to having an improved security stance and being able to bridge the gap between IT and the C-suite.
- **Look to third-party providers and independent assessments.** There are several reasons for looking to third-party providers and independent assessments. With the growing complexity of IT threats and technologies and tactics to avoid and mitigate them, it's becoming more and more difficult for individual enterprises to maintain the necessary levels of security expertise in-house. By utilizing expertise from third parties, your staff can focus on what you do best and outsource the rest. Further, it's important for assessments to be performed by independent third parties without skin in the game so that you can avoid bias.
- **Spend appropriately on what matters most.** Improved security doesn't come easy or free, and it also must be prioritized through proper data classification of critical assets. What matters most to your company's business and customers? This question can be answered through asset inventory and data classification efforts. Attaining the highest levels of security readiness requires investment in processes, tools, and technologies aimed at protecting the organization's crown jewels. The lesser — although still important — assets might be best protected through a managed security service provider, while the protection of the crown jewels remains internal. And the most security-ready organizations are investing in advanced tools such as advanced threat detection and mitigation solutions, vulnerability management, data security, web security and, in some cases, cloud application security brokers. The proliferation of SaaS, cloud, mobile, and bring-your-own-device platforms has reduced effectiveness of a perimeter defense strategy. Today, we must defend at all layers of the stack and both inside and outside the perimeter of an organization. Because we cannot afford to firewall every endpoint, SaaS, or cloud instance or every identity, we must identify the 20% of our business assets that are the most critical to defend and target spending appropriately.

CONCLUSION

IT security is a critical consideration to nearly every enterprise today, and having appropriate levels of security readiness should be top of mind for every board of directors and C-suite. And given the pervasive nature of cyberthreats today, organizations need to beware of falling into the overconfidence trap — thinking they are more secure than they really are.

Security progressive organizations, those with the highest levels of security readiness, are aware that they are being breached and are taking steps not to stop breaches, but to limit the damage of breaches to their organizations. They have the highest levels of investment, and their C-level executives are spending the most time and attention on security. Happily, they also have the best business outcomes, demonstrating that a focus on security can pay off.

Achieving security readiness starts at the top, with a commitment from senior management. CIOs and CISOs cannot go it alone; they need to educate their peers on the value of security to the business. They must make appropriate levels of investments and see to it that they have the right skills and processes in place — looking at both internal staff and third-party providers.

APPENDIX

Methodology

The information for this white paper came from IDC's January 2016 *Enterprise IT Security Readiness Index Survey,* sponsored by AT&T. IDC surveyed 802 members of senior IT and line-of-business executives in the United States, the United Kingdom, France, Germany, Japan, and Korea, with the responsibility for IT security solutions. The respondents came from organizations having 1,000+ employees across a broad range of industries. Survey respondents were asked about their security practices, solutions, and spending. In addition, they were asked about a variety of KPI metrics, enabling IDC to create an index linking IT infrastructure and organizational metrics to KPIs.

IDC developed the security readiness levels — progressive, proactive, reactive, and passive — using the following methodology:

1. Responses to all questions in the survey were scored on according to four-point scale characterizing their "readiness" to deal with cybersecurity incidents. For example, for the question "What job title is responsible for IT security?" organizations in which higher job titles were responsible for IT security received a higher score than those in which lower job titles were responsible.
2. IDC performed statistical analysis to identify questions best correlated to positive business outcomes. For example, the question "What has been your increase in security spend from 2015 to 2016?" has a high correlation to the measured business outcomes.
3. IDC then selected a subset of 15 questions with the highest statistical correlation that also covered a representative set of security policies and practices.
4. IDC created a readiness scoring histogram for all responders for the 15 questions to identify and score ranges for the four levels of security readiness, and identified natural cutoffs based on mean and standard deviations.

The survey was supplemented with a focus group of U.S. CIOs and CISOs to help validate and vet key assumptions as part of the survey development process.

Note: All numbers in this document may not be exact due to rounding.

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-community.com
www.idc.com