A Forrester Consulting
Thought Leadership Paper
Commissioned By Trend Micro

October 2014

21st Century Threats Demand 21st Century Security Approaches

Forward-Thinking Security Pros Will Guide Their Organizations To A Secure Future

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Welcome to the golden age of hacking. This is the reality that businesses operate in today. An amalgamation of legacy and new technology systems and processes, traditional approaches to information security, and explosion of growth in data collection is pushing enterprises to a breaking point. Hardly a week goes by without news of a data breach discovery — often one where attackers have had access for a long period of time. Targeted attacks and advanced threats are becoming the norm. Stakeholders from across the enterprise are tuning in and recognize that data protection is paramount, yet security leaders continue to face challenges adapting to today's threats, protecting their data, and articulating the value of security investments.

In June 2014, Trend Micro commissioned Forrester Consulting to evaluate a shift in roles and priorities in IT security budgeting and decision-making in the wake of increased prevalence of and attention to targeted attacks and advanced threats. More specifically, Trend Micro sought to understand how IT security professionals should position themselves and their responsibilities in the context of data loss risks. Then, to further explore this trend, Forrester developed a hypothesis that tested the assertion that enterprises must rethink the value of security, focusing not on return on investment (ROI) but on return on risk reduction, and that security professionals must move into a new role of trusted advisors on such matters for the organization.

The threat landscape has changed, and security professionals need to help their organizations catch up to the reality.

In conducting a survey of 220 IT security professionals with responsibility for planning and strategy against targeted attacks and advanced threats, Forrester found that many have been victims of targeted attacks. While companies demonstrate willingness to increase security budget, firms still struggle with business justification for new security investments. Adding to the complexity, the number of stakeholders from across the organization who are involved in security investment decision-making is also increasing. It is an opportune time for security professionals to step up into a greater leadership role with a goal of elevating and treating security as a business imperative and not a cost center.

KEY FINDINGS

Forrester's study yielded four key findings:

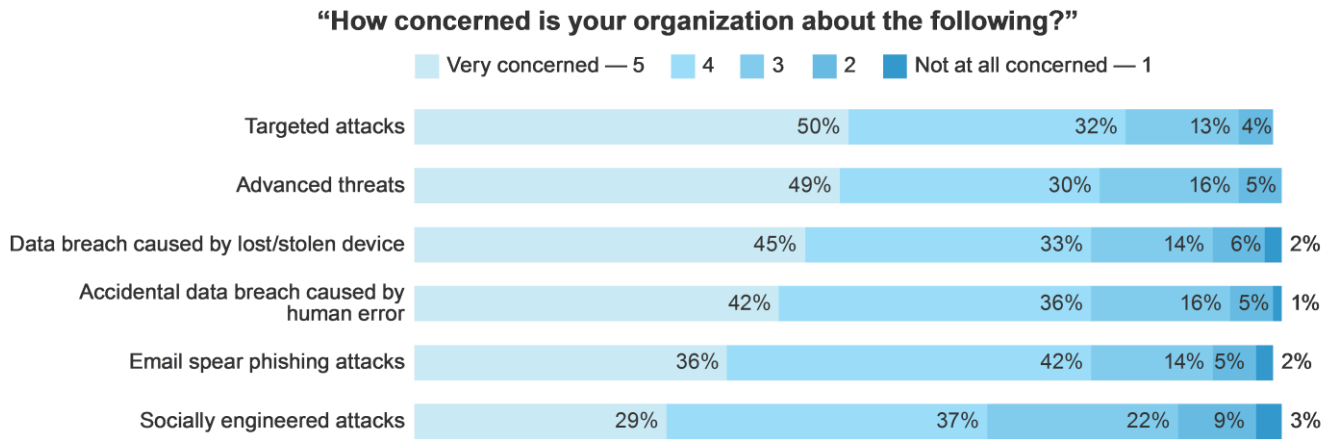
- **Targeted attacks and advanced threats represent major risk to organizations.** A majority of the organizations we surveyed have been the victim of a targeted attack or advanced threat. These modern threats are gaining attention within their organizations, representing the No. 1 and No. 2 IT security concerns, due to potential repercussions such as data loss, intellectual property theft, and reputational damage to their brand. At the same time, IT security budgets are increasing, with no respondents reporting a decrease.
- **Firms are not budgeting for modern security risks.** Survey respondents reported big challenges in justifying security investments due to the changing nature of IT threats and a lack of understanding of modern security risks. The increasing number of stakeholder groups from around the organization involved with budgeting processes further complicates efforts to get the right protections in place.
- **Many organizations don't treat their data with the respect it deserves.** Regulatory compliance still constitutes the main driver for determining the value of data, potentially leaving a lot of vulnerability and putting the business at serious risk.
- **Security professionals have the opportunity to play a key role in preparing their organization for the modern threat landscape.** IT security professionals from a variety of industries and company sizes reported increased involvement in strategic business decisions related to data protection and other security concerns. With a conscious effort, these professionals have the opportunity to become trusted, sought-out advisors and move beyond the old tactical approach to security.

Targeted Attacks And Advanced Threats Are Ubiquitous, And Organizations Are On Alert

It often seems that barely a week goes by without another corporation announcing a major data breach — a few million social security numbers here, tens of millions of credit card numbers there. Targeted attacks, which Forrester defines as attacks in which a threat actor is targeting the security defenses of a specific organization, and advanced threats, defined as a continuous hacking process often utilizing malware to exploit system vulnerabilities, are a big problem. In 2013, a roundup of publicly reported security incidents and breaches reported 873 targeted attacks versus just 79 broad attacks.[1] For the companies that fall victim, the aftermath is messy, to say the least. Unfortunately, most breaches are also discovered by a third party, such as customers, law enforcement, computer security incident response teams (CSIRTs), and threat researchers, and not the breached company itself, which adds to the embarrassment and public perception that enterprise security is lacking.[2] Given the high profile of these events and their obvious ramifications, it's difficult to ignore their severity. Indeed, security professionals, as well as the larger organization at most companies, are taking note, often due to personal experience.

- **Most firms are experiencing threats firsthand.** Incidents of targeted attacks and advanced threats aren't limited to the ones we're all used to hearing about on the news these days. In fact, a full 62% of survey respondents indicated that their organization has experienced such an event. Particularly vulnerable are certain industries such as financial services and telecommunications, where 66% and 70%, respectively, reported being victims. Three percent reported being unsure of whether or not their organizations have been a victim, but this figure shoots up to a concerning 11% among companies with more than 20,000 employees, the largest segment we surveyed, highlighting a challenge that is particularly pertinent for those organizations likely to have the most at stake.
- **Concern is rising among IT professionals.** Given their pervasive nature, it comes as no surprise that modern security risks are top of mind among IT professionals. In fact, targeted attacks and advanced threats top the list of six security concerns we surveyed on. 82% ranked their organization's level of concern around targeted attacks at a "4" or "5" (on a five-point scale), with 79% indicating the same for advanced threats (see Figure 1). 87% reported an increase in this concern within their companies over the past 12 months. Respondents recognize the severity of the various ramifications of these new breeds of IT risks, but they are particularly worried about losing their

FIGURE 1
Targeted Attacks And Advanced Threats Top The List Of IT Security Concerns



Note: Percentages may not total 100 due to rounding.

Base: 220 senior IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

customers' data (and accompanying trust), as well as the broader damage to their brands and the exposure of their intellectual property (see Figure 2).

› **Security budgets are growing.** Unsurprisingly, firms are responding to the increased risk of attacks by growing their IT security budgets. In the aggregate, 78% of all survey respondents anticipated an increase in security technology and solution budgets over the next year, with a fifth forecasting rates of increase in excess of 10%. Among organizations that have fallen victim to attacks, the numbers are even more impressive. 25% of such firms anticipate increases of more than 10%. Large organizations (with more than 20,000 employees) also report greater than average increases, with 27% anticipating rates of growth exceeding 10% (see Figure 3).

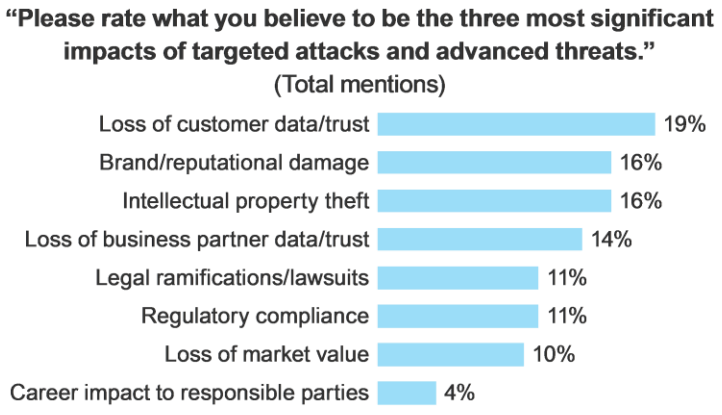
Antiquated Perspectives And Shifting Organizational Dynamics Complicate The Fight Against Modern Threats

Although companies appreciate the unprecedented hazards presented by targeted attacks and advanced threats, and are for the most part responding with increased security budgets, major challenges remain in adequately protecting organizational data. Relics of old approaches to security budgeting are alive and well, yet they don't mesh well with the realities of today's market in which value and risk must be evaluated in a new light. Combine this with an increasingly crowded decision-making cadre, and the process of justifying an investment that protects against very real dangers isn't so cut-and-dry. Specifically, we found that:

› **Firms struggle to appreciate modern risks.** Despite widespread reported increases in budgets, many security professionals still face a heady task when proposing security investments. Our survey results suggest a particularly difficult task of adjusting to today's threat landscape and conveying the danger of confronting it with existing tactics. 67% and 55% rated "changing/evolving nature of IT threats" and "lack of understanding of security risks," respectively, at a "4" or "5" (on a five-point scale)

FIGURE 2

Firms Fear Tarnished Reputations And Diminished Customer Trust

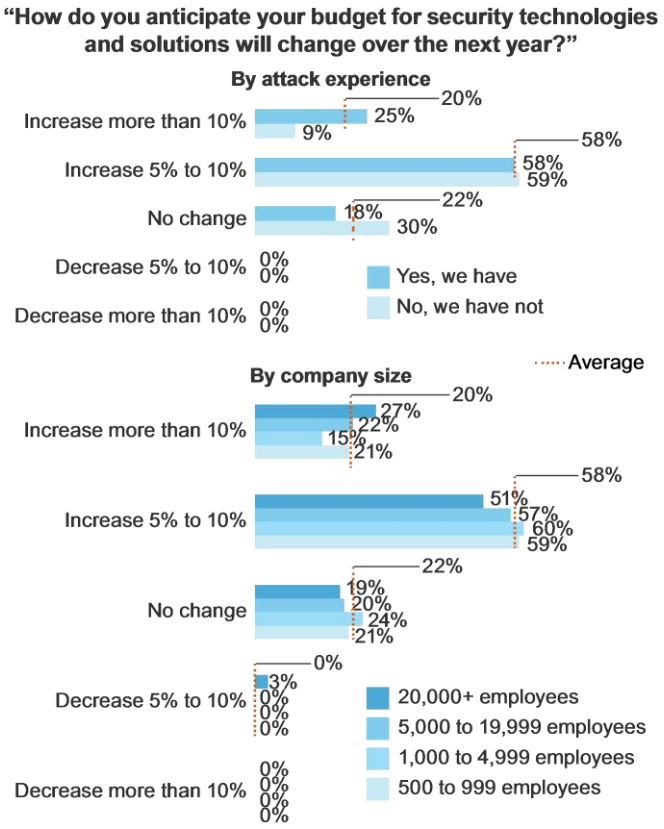


Base: 220 senior IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

FIGURE 3

Security Budgets Are Rising Across The Board, With Attack Victims And Large Companies Leading The Charge



Note: Note: Percentages may not total 100 due to rounding.

Base: 220 senior IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

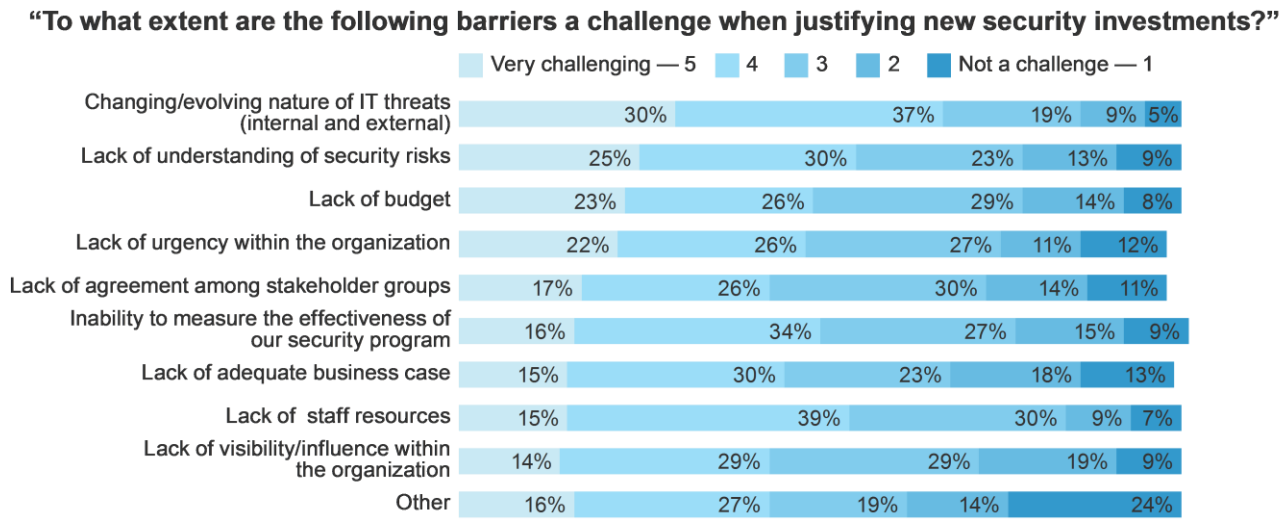
when asked to evaluate the level of challenge present when justifying new investments (see Figure 4). These constitute the most difficult to overcome among the barriers we asked about. Failing to proactively protect themselves isn't the only way organizations are putting themselves at risk, however. Currently, 39% lack first-party cyberinsurance and 51% are without third-party liability cyberinsurance, thus leaving them vulnerable to extensive financial and legal accountability in the event of a breach. While insurance will certainly not cover the cost of a breach, it may help to offset and mitigate a portion of it in a time when any and all safeguards make a difference.

› **Motivations to secure data remain myopic.** When asked how their organization determines the value of data to their company, the largest group (66%) assigned the most influence to data being subject to compliance. Although maintaining compliance is critically important as part of a comprehensive data security strategy, it's only one piece of the puzzle. In an era with increasing scrutiny over consumer data use and applications, the types of data that fall under regulation are increasingly nebulous, making compliance requirements an unreliable and insufficient point of reference.[3] Furthermore, after personally identifiable information (PII), intellectual property (IP) is the second most compromised type of corporate data.[4] Beyond the public relations and brand damage of customer data theft, the consequences of IP leaks are potentially devastating to a company's competitiveness and market standing.[5] Companies, therefore, are leaving a lot of valuable data on the table when they concentrate exclusively on regulatory compliance, particularly in an era of susceptible storage techniques and fleeting understanding of data use policies.[6]

› **Security stakeholder groups are multiplying.** It's been said that security is everyone's responsibility. While true, it takes effort to maintain this mindset and culture within the organization.[7] Between internal efforts and an increased awareness thanks to media coverage of data breaches, the importance of security to various departments and functions is being realized. As a result, non-IT departments are increasingly contributing to security budgets. Survey respondents reported an average of only 52% of their total security budgets being from IT itself, leaving nearly half to be sourced from elsewhere in the organization. Average rates of involvement of non-IT departments range from 24% of procurement departments up to 41% of privacy groups. Not only is this phenomenon prevalent, but it's increasing. No fewer than 55% of respondents reported an increase in decision-making involvement from a given department outside of

FIGURE 4

Firms Struggle To Adjust To Evolving Threats



Note: Percentages may not total 100 due to rounding.

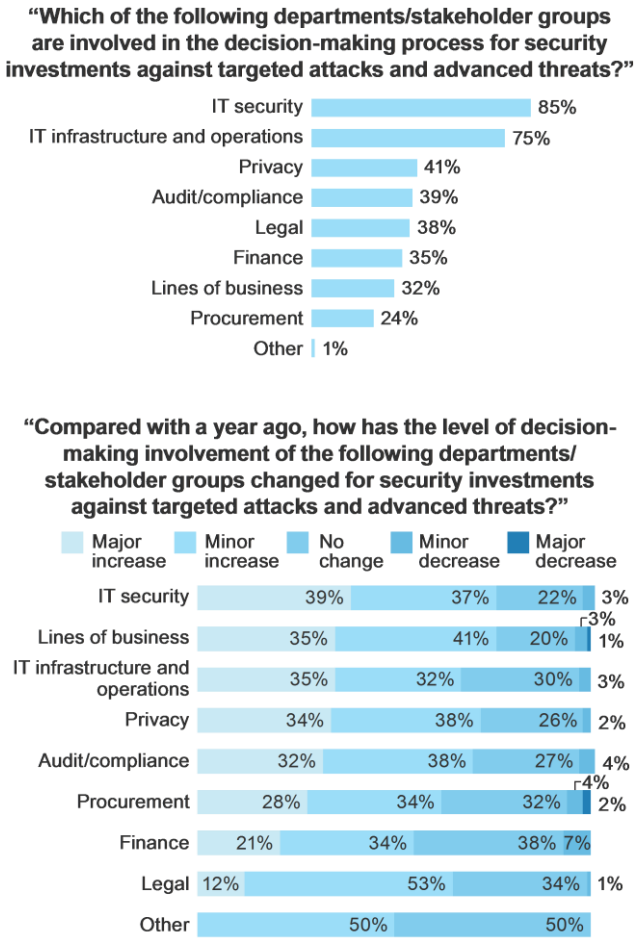
Base: 220 senior IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

IT (see Figure 5). However, balancing the priorities and perspectives of these disparate parties adds yet another potential setback at a time when taking action has never been more critical.

FIGURE 5

Security Budgeting Involves An Increasing Number Of Stakeholders



Note: Percentages may not total 100 due to rounding.

Base: 220 senior IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

Leverage Security Prowess To Educate And Evolve Your Wider Organization

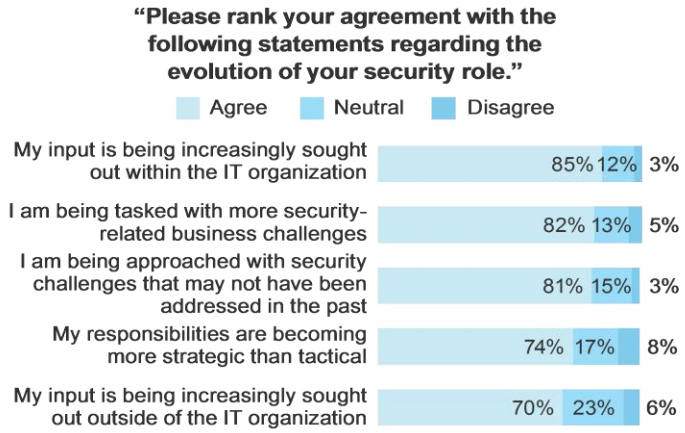
Clearly, the road to an enlightened approach to security budgeting has some considerable obstacles. However, there are plenty of reasons to be optimistic. Although organizations have some catching up to do when considering how to combat today's IT risks, the old line of reactive thinking is breaking down, and organizations are starting to look at security more holistically. Security professionals have the chance to do more than just adapt to changes. Rather, they can fundamentally shift their role in their organizations into a strategic asset, rather than a tactical necessity. To maximize this opportunity, proactive security professionals in forward-thinking organizations will:

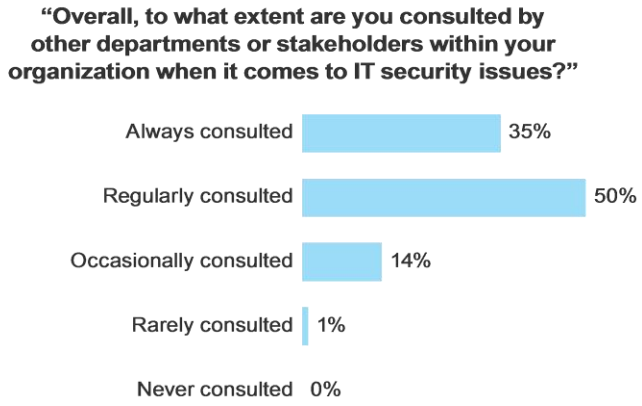
› **Treat security as the business imperative that it is.** In the age of the customer, every organizational function — even those that have historically been considered "behind the scenes" — directly and visibly influence whether or not a group or individual decides to do business with a company.[8] For security professionals, this means adopting and implementing new technologies and processes more quickly than ever before to maintain customer trust while providing the capabilities they demand. This is a lofty but necessary goal that's simply impossible to achieve with old approaches to security. Fortunately, security professionals show signs of embracing this mentality. "Reputational risk" is the second most cited justification for investment in security technologies or solutions among our survey respondents, and "loss of customer data/trust" is considered the No. 1 impact of targeted attacks and advanced threats. As security professionals, themselves, take on this business-minded approach, so too does the business trust them with related tasks: 82% of survey respondents said they are being tasked with more security-related business challenges and 70% are being sought outside of the IT organization.

› **Take the helm as trusted security advisors to the organization.** Shifting to a business mindset isn't the whole equation to evolving security's role. Security professionals need to position themselves as *strategic*, as well. For example, ensuring during development that a product or service is secure has a much bigger impact than patching a vulnerability once it's been downloaded by millions of users. Luckily, this is another area in which

FIGURE 6

Security Professionals Have The Opportunity To Take A Strategic Business Role In The New Paradigm





Note: Percentages may not total 100 due to rounding.

Base: 220 Senior IT security decision-makers

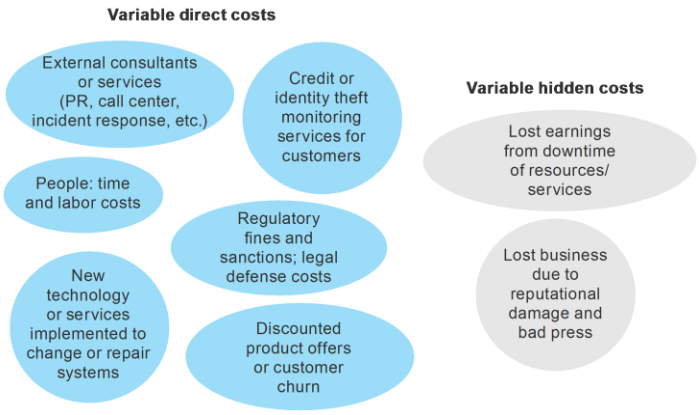
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

the tide is shifting, according to our survey. Nearly three-quarters of respondents reported that their responsibilities are becoming more strategic than tactical, and 99% reported being at least occasionally consulted by other departments on security issues. The attention is from high up, too. Outside of IT, C-level executives and boards of directors are the two groups most often reached out to by security staff to discuss solutions and processes. Room for improvement always exists, however, as only 35% reported being "always consulted" (see Figure 6)

› **Move beyond "cost consequence" mentality.** For too long, businesses have been driven to act due to a negative stimulus that necessitates a response, such as a breach event or failed compliance audit. Some, after risk analyses, also make calculated choices to not invest in security, opting to pay fines instead should an incident occur, believing that this approach is more cost-effective. In reality, there are myriad direct and hidden costs resulting from a data breach that overshadow the cost of implementing the right technology and processes. What's more, these costs are far and away more difficult to recover and take a great deal of time and effort to manage (see Figure 7). Lawsuits, for example, can have timelines that stretch upwards of ten years and incur millions of dollars in legal fees and plaintiff damages, and recent data breach court sagas have upped the ante for companies.[9] In addition, fast-evolving and changing global data privacy laws have upped the ante for penalties.[10][11] In some Asian countries, for example,

FIGURE 7

Several Direct And Hidden Costs Are Associated With A Data Breach



Source: "The Cybercriminal's Prize: Your Customer Data And Competitive Advantage," Forrester Research, Inc., August 6, 2014

criminal prosecution and jail time for executives on top of fines is also a possibility.[12] Luckily, survey respondents also show a turning tide of attitudes. When asked of the top ways in which their organization articulates the value of IT security investments, most agreed with the statement: "We believe protection of customer data is corporate social responsibility," with the aim of protecting their brand reputation a close second.

Key Recommendations

Forrester's in-depth survey of IT security professionals yielded several important recommendations:

- **Take the steps needed to become a strategic asset.** Security pros have the opportunity to become a strategic advisor to the business. In order to do so, they have to move away from the old ways of doing security work to build a level of confidence necessary to become a critical asset. Study how your business works and what the stakeholder objectives are. Seek out allies within the business who can support and inform you on this journey. Consider enlisting the input of partners from outside your organization with the experience and expertise in such efforts to help navigate this new territory. With the right approach, you'll earn more input on security decisions.
- **Evangelize the importance of data protection.** It's all about the data, and unfortunately a large majority of breaches are discovered by a third party. Demonstrate to your technical colleagues how critically your company's board and executive team think of data protection, and become an advocate for the right steps your organization must take to assure their confidence that the organization can detect breaches and anomalous activity.
- **Give your company a reality check on modern risks.** Broaden the organization's thinking on the potential impact of targeted attacks. These days, the implications are much more than malware on the network. Just because you're in purchasing, managing a kiosk, or don't have "security" in your job title doesn't mean you can't be a proactive force in minimizing your company's risk through your own behaviors.
- **Move beyond cost consequence mentality.** Traditionally, security budgets and ROI are calculated around probabilities, an approach that just doesn't work in the context of today's digital risks. Beyond rethinking the risks themselves, address disparate stakeholder concerns that mirror expanded buying circles and articulate the importance of the right protection to those in sourcing. Make the effort to demonstrate how investing today can help avoid much bigger headaches down the road, in addition to supporting and enabling critical business initiatives.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 220 IT security professionals with responsibility for their organizations' planning and strategy for targeted attacks and advanced attacks to evaluate a shift in roles and priorities in IT security budgeting and decision-making in the wake of increased prevalence of and attention to targeted attacks and advanced threats. Survey participants included decision-makers in security oversight, information risk, security architecture and engineering, and security operations. Questions provided to the participants asked about their organization's IT budgeting processes and priorities, changes in concern around various IT security threats, and the evolution of their job responsibilities in the broader organization. Respondents were offered a small incentive determined by their survey panels as a thank you for time spent on the survey. The study began in June 2014 and was completed in October 2014.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"The Cybercriminal's Prize: Your Customer Data And Competitive Advantage," Forrester Research, Inc., August 6, 2014

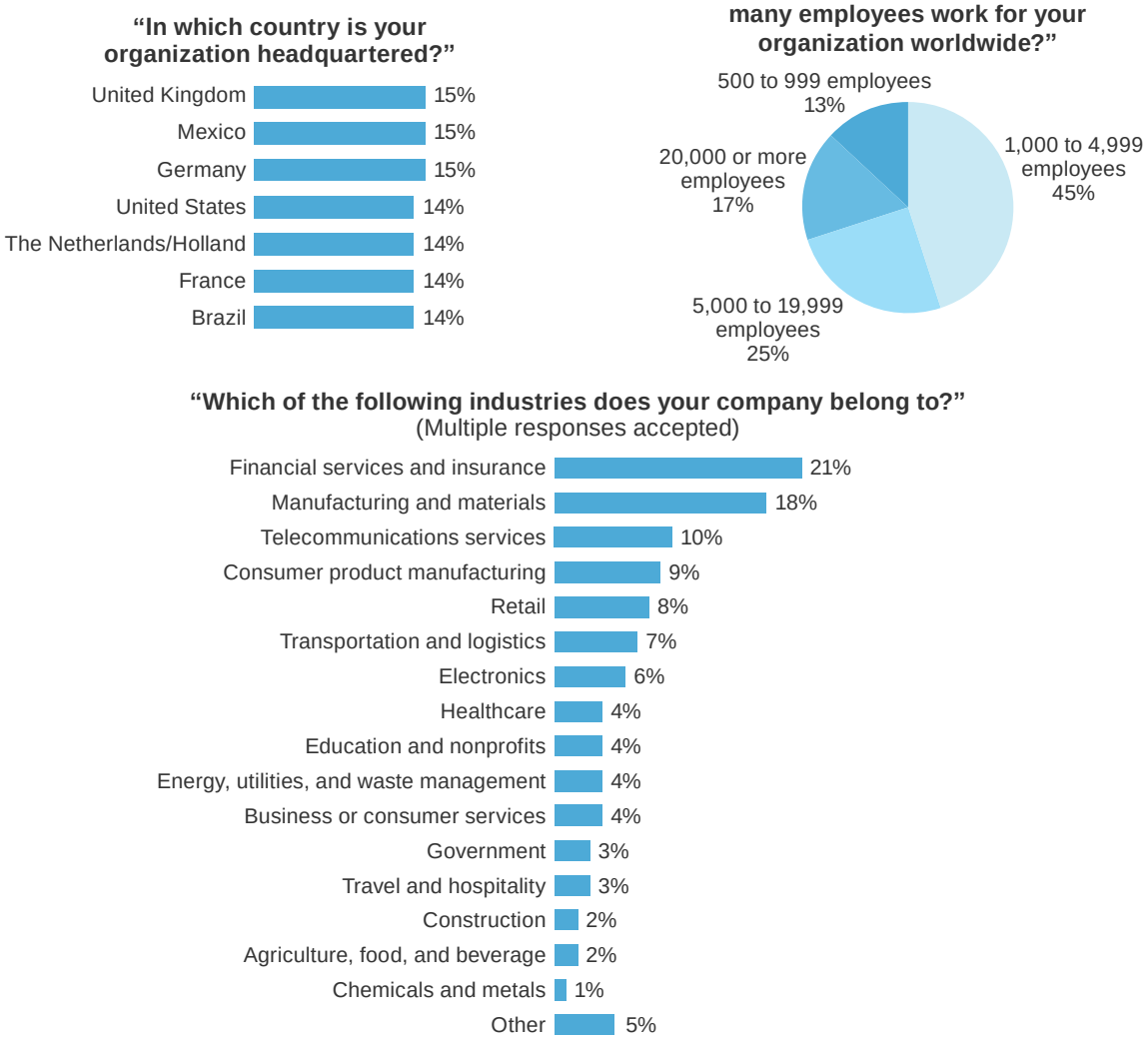
"Evolve To Become The 2018 CISO Or Face Extinction," Forrester Research, Inc., August 20, 2014

"Security Needs To Accelerate Into The Age Of The Customer Or Risk Marginalization," Forrester Research, Inc., May 16, 2014

"Understand The State Of Data Security And Privacy: 2013 To 2014," Forrester Research, Inc., October 1, 2013

Appendix C: Demographics/Data

FIGURE 8
Respondent Demographics



Note: Percentages may not total 100 due to rounding.

Base: 220 Senior IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, July 2014

Appendix D: Endnotes

[1] Source: “Introducing Forrester’s Targeted-Attack Hierarchy of Needs, Part 1 Of 2,” Forrester Research, Inc., May 15, 2014.

[2] In a 10-year analysis of breach discovery methods, a 2014 benchmark report on data breaches showed that third parties continue to be a main source of breach detection. However, the report notes that it is encouraging that internal discoveries are slowly making progress. Source: Verizon (http://www.verizonenterprise.com/DBIR/2014/).

[3] As of September 2014, the US Congress is considering 112 pieces of legislation addressing privacy and data breaches, and the EU Commission is preparing to significantly tighten data regulations in an update to its 1995 Data Protection Directive. The state of California also recently passed its own series of laws on data governance. Source: “How Dirty Is Your Data?” Forrester Research, Inc., September 16, 2014.

[4] Source: Business Technographics Global Security Survey, 2014, Forrester Research, Inc.

[5] See this report for examples of intellectual property attacks and how they have an impact on victim companies. Source: “The Cybercriminal’s Prize,” Forrester Research, Inc., August 6, 2014.

[6] Forrester’s Forrsights Devices And Security Workforce Survey, Q2 2013, found USB flash drives and CD/DVDs as the most commonly used method for file storage and access among information workers. The survey also found that only 55% of information workers are aware of and understand policies in place for data use and handling. Source: “Understand The State Of Data Security And Privacy: 2013 To 2014,” Forrester Research, Inc., October 1, 2013.

[7] Too many security professionals describe their model as "everyone's accountable" and expect that this shared accountability will translate into compliance and due care for every staff member all the time. Unfortunately, scientific studies show that sharing accountability commonly has the *opposite* outcome. Reevaluate your current security model to create specific guidelines and clear action steps so that policies become a crucial foundation that will affect not only your security program but your employees, business partners, and overall organizational security culture. Source: “Enforce A Just Culture To Fortify The Human Firewall,” Forrester Research, Inc., April 24, 2014.

[8] Forrester defines the age of the customer as a 20-year business cycle in which the most successful enterprises will reinvent themselves to systematically understand and serve increasingly powerful customers.

[9] See this report for examples of recent lawsuits related to data breaches. Source: “Brief: Legal Costs In A Customer Data Breach Now Pack A Bigger Punch,” Forrester Research, Inc., June 19, 2014.

[10] To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. Due to the dynamic nature of data protection legislation, information within the interactive tool is kept up-to-date with an annual update cycle. Source: “Forrester’s 2014 Data Privacy Heat Map,” Forrester Research, Inc., August 6, 2014.

[11] While data protection requirements in the US are commonly industry-centric, those in the EU focus more on the individual's right to privacy. This leads to a number of differences in how data should be handled in the EU as opposed to the US, especially in transferring data between countries of varying regulatory standards. This report is an update to the report of the same name published on September 16, 2011 as part of Forrester's commitment to keep our clients up-to-date on the rapid pace of privacy regulation reform. Source: “Q&A: EU Privacy Regulations,” Forrester Research, Inc., March 12, 2014.

[12] Across Asia, data privacy laws are fragmented, and the regulatory environment is different for each jurisdiction. Significant penalties mean that compliance is not optional and specific focus is required to remain within the legal boundaries. This study highlights key data privacy regulations from across the Asia Pacific region and presents best practices for staying on top of these evolving requirements. Source: “What You Must Know About Data Privacy Regulations In Asia Pacific,” Forrester Research, Inc., May 15, 2013.