BUILDING A BETTER BUDGET FOR ADVANCED THREAT DETECTION AND PREVENTION: *AN IANS CUSTOM REPORT*

SEPTEMBER 2014

Sponsored by:

Contents

Contents 2
Executive Summary 3
Top Cyber Threat Concerns 4
The State of the Security Budget 6
Building a Better Security Budget 7
Looking Forward 11
About FireEye 13
About IANS 13

Executive Summary

The attackers of today are more sophisticated than ever, and we know this from a wealth of evidence related to data breaches and other incident scenarios seen in recent years. Advanced malware and attack techniques are becoming more common all the time-- and organizations are struggling to keep pace.

The 2014 Verizon Data Breach Investigations Report (DBIR)[1] illustrates just how rapidly information security is changing, particularly in the retail industry. The now infamous Target breach increased awareness around the vulnerabilities present in Point of Sale (POS) systems. These POSs were exploited as a new target for attackers in 2013 looking to exploit large retail organizations. The DBIR describes details of 198 data breach intrusions that led to data disclosure.

Explosive growth in "crimeware" was also noted, which specifically targets identification credentials, banking information, and payment information. Most crimeware is installed via "drive-by downloads" and Trojan downloads in seemingly innocent applications. Verizon also noted a significant increase in cyber espionage, which they define as incidents that "include unauthorized network or system access by state-affiliated actors". In other words, this is in reference to the installation of malware to spy on government employees and organizations; however Verizon is quick to note that they do not yet have complete data sets on these kinds of attacks. Even then, they reported 511 cyber espionage attacks, with 306 confirmed cases of data disclosure. Notably, most of these attacks originated from malware in email attachments and through drive-by downloads. Mandiant's 2014 M-Trends report[2] noted some additional attack vectors that threat actors used to successfully breach organizations in 2013. First, attackers are now simply buying access to systems previously compromised by botnets, thus shortening the initial attack cycle dramatically. In addition, third-party vendors who were connected to the target organizations were often compromised to gain initial access, as well, forcing organizations to revisit supply chain security policies and controls for all connections into their networks.

Information security teams are realizing that they need new tools and techniques to combat the sophisticated security threats of today. With that realization, however, security organizations are struggling to develop budgets and make successful business cases for purchasing more capable tools that can help stem the tide of advanced threats and attacks. Currently, many security decision makers have a budget that is 15% or less of the overall IT budget. Should it be more? And if so, what should the priorities be?

IANS recently conducted an independent survey of 100 security decision makers and influencers across a variety of global organizations, nearly 75% of who are in management and executive roles, with the other respondents acting in technical leadership positions. Almost half of the respondents are in organizations with over 10,000 employees, with the other half ranging in size from 500 to 9,999. 7% of respondents have a small security team of 1-3 people, 29% have 4-10 people, 23% have 11-20 people, and 41% have more than 20 people in their security

[1] http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

[2] https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

organization. Many of the questions we asked allowed for multiple answers, so some charts and graphs show responses that add up to more than 100%.

This report will examine the following:

- The specific threats organizations are focused on, in addition to *how* data breaches have been executed and *what* the major effects of those breaches have been.
- The current state of security budgets, as well as changes and challenges in budgeting approaches
- How many organizations are planning to replace security technologies with new products that more effectively combat advanced threats
- The types of security tools being replaced and those slotted for inclusion in new security designs that more effectively combat advanced threats.

The conclusion will reveal how security teams are developing successful business cases and influencing business decision makers.

Top Cyber Threat Concerns

Given the targeted nature of attacks today and the proliferation of sophisticated malware and data breach scenarios, what are the top cyber threats that most security teams are concerned with? In our survey, financial crime and fraud were the top issues cited by security professionals, followed by insider threats and state-sponsored cyber espionage. Several other responses included generic "script kiddie" attacks from outside the network, as well as data loss. These results are shown in Figure 1:

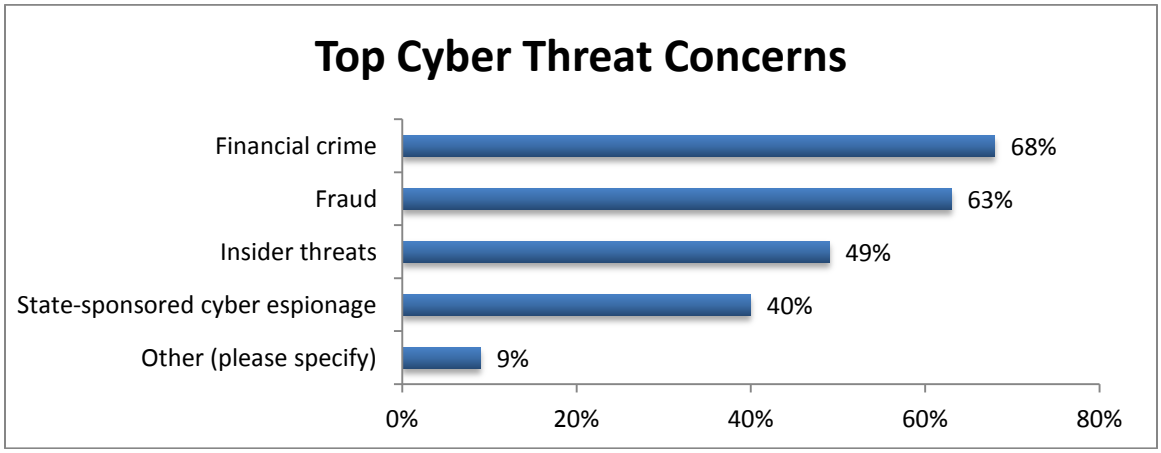

Figure 1: Top Cyber Threat Concerns

To better understand the respondent's perspective, we asked how many of them had experienced a security breach:

- 37% of respondents said they had
- 51% asserted that they had not
- 12% were indefinite (likely due to the stealthy nature of today's attacks)

For those that had:

- 81.1% indicated that the breach involved malware and/or sophisticated adversaries
- 13.5% stated that their breach scenarios did not include advanced malware or adversaries
- 5.4% were not sure at this point in time

The above results support many of the trends reported in the Verizon DBIR and other industry news sources. Today's attacks are increasingly due to more sophisticated attackers, and are still primarily accomplished via installation of complex malware. Once data breaches occur, the range of impact is broad and varied across industries. IANS asked those respondents who had experienced a breach what the impacts of the breach were on their business. The results are shown in Figure 2 (with multiple responses possible):

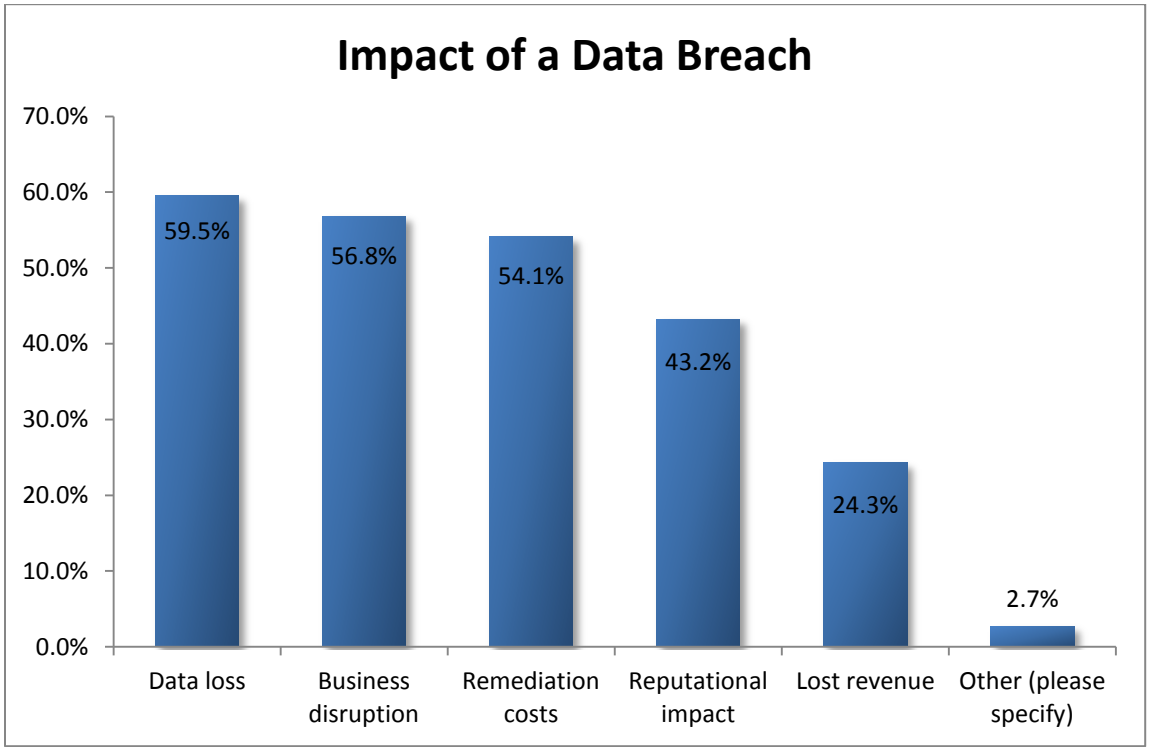

Figure 2: Impact of a Data Breach

The results conclude that the primary impact of a data breach is data loss (59.5%). Business disruption and remediation costs follow closely, however, which reflects the severity and impact of data breaches on many organizations. As more organizations rely on information technology as business-critical systems, loss of trust in those systems can lead to significant damages, ranging from outages to reputational impact due to breach disclosure. Today's breaches tend to be bigger, more widespread, and harder to determine root cause due to the sophistication level of attackers. It's not surprising that most of the costs incurred from data breaches come from investigation, loss of business from lack of customer or industry confidence, and later, cleanup.

The State of the Security Budget

Given the sophistication of today's attacks, do most organizations have the appropriate security budgets? According to survey responses, 46% believe the answer is "yes". 33% felt that their security budget was not adequate, and another 21% were uncertain. 59% indicated that their security budgets were increasing, though, with only 5% seeing their overall security budgets decrease. 36% stated that their budget was remaining the same at this time. With most budgets increasing or remaining static, where then do security budgets fall in terms of the overall percentage of information technology budget? Figure 3 depicts the breakdown of responses:

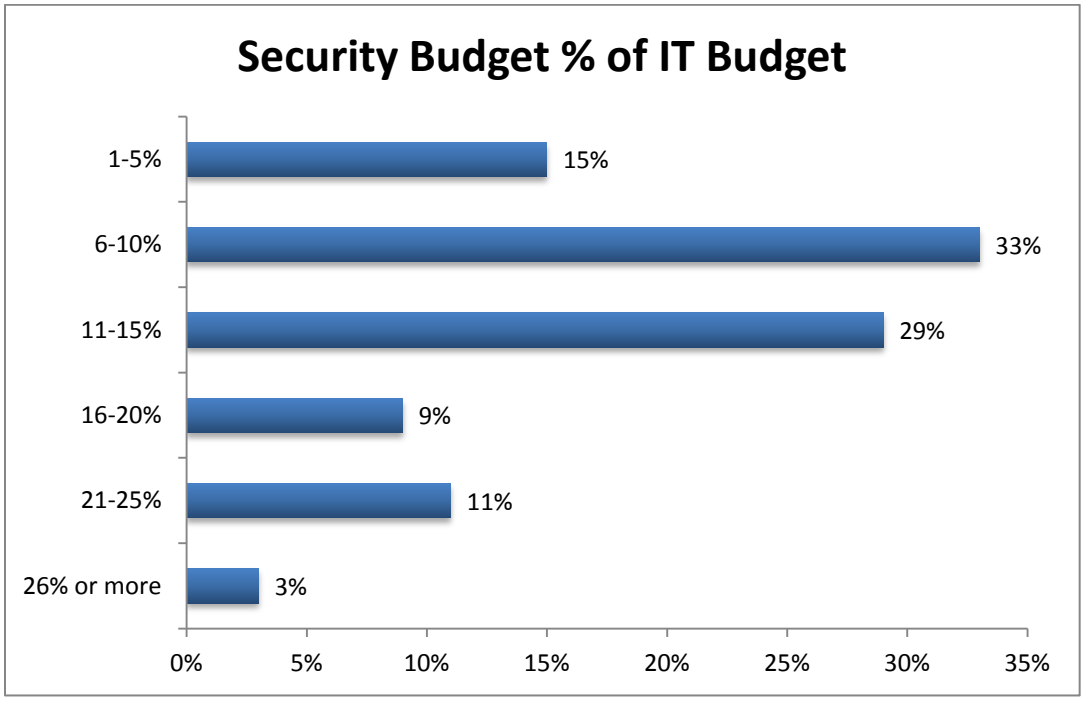

Figure 3: Security Budget Percentage of IT Budget

Most responses fall in the 6-15% range, which is a positive trend as many organizations have traditionally had a security budget that was 5% or less of the overall IT budget. Nine percent of responses fell in the 16-20% range, with 11% coming in at up to 25%. Only a very small number of organizations are spending more than 25% of their IT budget on security. IANS asked those respondents who indicated that their overall security budget was increasing whether the money was earmarked for a particular type of security technology. 40% of respondents indicated that additional budget was, in fact, planned for specific tools. So what are these security teams planning to purchase with the additional budget? Figure 4 shows the breakdown:

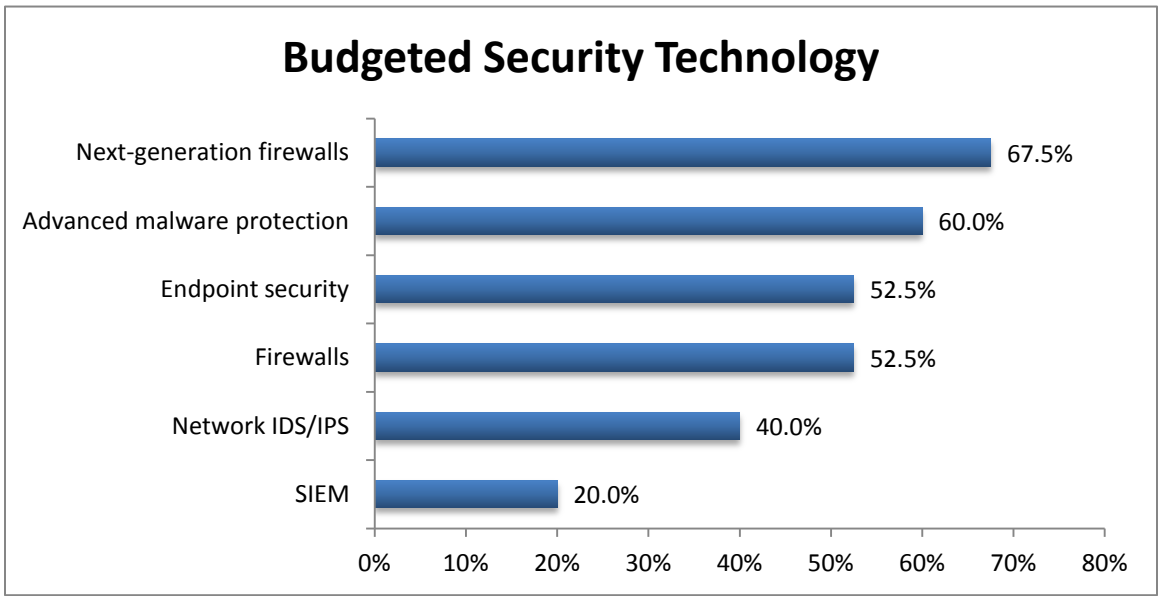

Figure 4: Newly-Budgeted Security Technology

What do these responses indicate? First, it is obvious that most organizations have more than one new security technology initiative underway. Many survey respondents indicated that they are budgeting for several technologies at the moment. Not as many organizations are looking to purchase SIEM tools, which likely indicates that many already have a solution in this area. Solutions focused on monitoring and blocking threats and attacks at the network and host levels (network IDS/IPS and endpoint security) are budgeted by 40% and almost 53%, respectively, which may indicate new tools or replacement projects for these common security controls. The fact that 52.5% of respondents are planning to spend on traditional firewall technology came as a bit of a surprise, although this may indicate that organizations are simply upgrading to newer models or replacing equipment that is nearing end-of-life. What was not surprising was the high number of responses indicating plans to acquire advanced malware protection and next generation firewall technologies (60% and 67.5% respectively). Such technologies offer enterprise security teams the most capabilities for detecting sophisticated malware and command-and-control channels on the network, both of which are hallmarks of the advanced attacks seen today by many.

Building a Better Security Budget

Every security team wants a higher budget for technology and projects. So how do successful teams go about advocating for additional budget? Figure 5 shows some of the common responses:

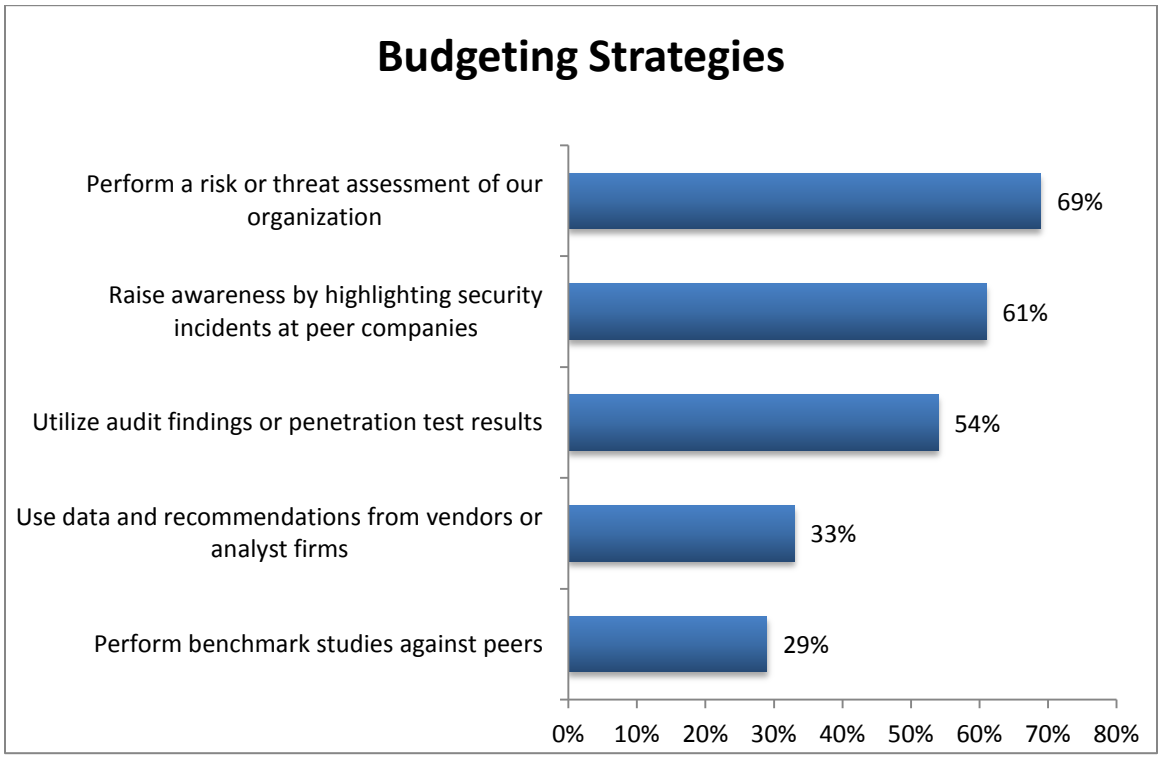

Figure 5: Strategies for Advocating for Additional Security Budget

The most common strategy for improving budgets (based on 69% of responses) was to perform a risk or threat assessment within an organization. Exposing the vulnerabilities and potential weak points in the IT operations and architecture of the business is an effective way to demonstrate where gaps exist. In-depth penetration tests and audits were another successful method for demonstrating risk, and 54% of respondents were able to leverage results from audits and pen tests to help improve security budgets. 61% of respondents were also successful in improving security budgets by highlighting security incidents at peer companies which helped raise the level of awareness with executives and business stakeholders. A third of the respondents leveraged data and recommendations from vendors and analyst firms when seeking additional budget, and 29% performed benchmarking studies against peers.

We asked respondents whether they planned to replace any of the main security technologies that they relied on. Most said no (55%), with some undecided (34%) and only 11% who indicated that they definitely would be replacing something. For those that planned to replace technologies, the most common solutions being replaced were traditional firewalls, SIEM, and antivirus. 53% of respondents also indicated that they had already purchased solutions focused on preventing or responding to advanced attacks. Of these organizations, most noted that the budget for these solutions had come from IT operations (54.7%), with the traditional security budget coming in second at 52.8%. Risk management (20.8%) and compliance (5.7%) rounded out the responses, shown in Figure 6:

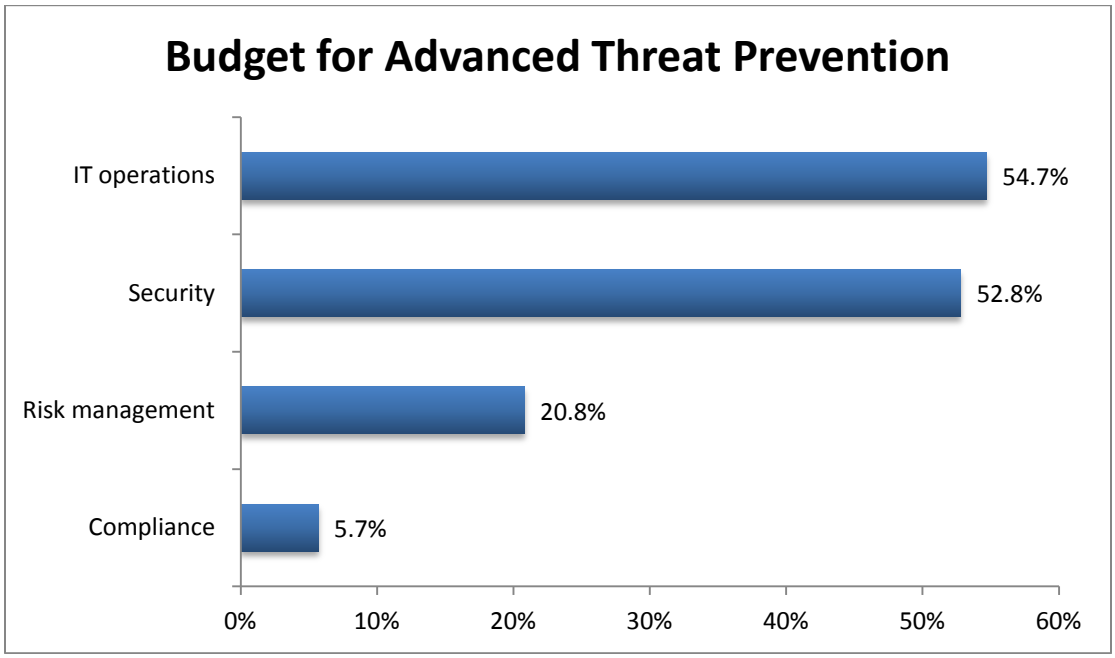

Figure 6: Budget Paying for Advanced Threat Detection/Prevention

Are more organizations developing budgets for advanced threat protection and/or incident response? Currently, 51% of organizations are allocating budget dollars for these areas specifically. Many organizations are still struggling to get a definitive budget allocation for advanced threat protection due to a variety of reasons. The biggest challenge seems to be competing IT priorities (73%), followed by competition with other business priorities (40%). Competing security priorities and lack of concern from management were less common, as shown in Figure 7:

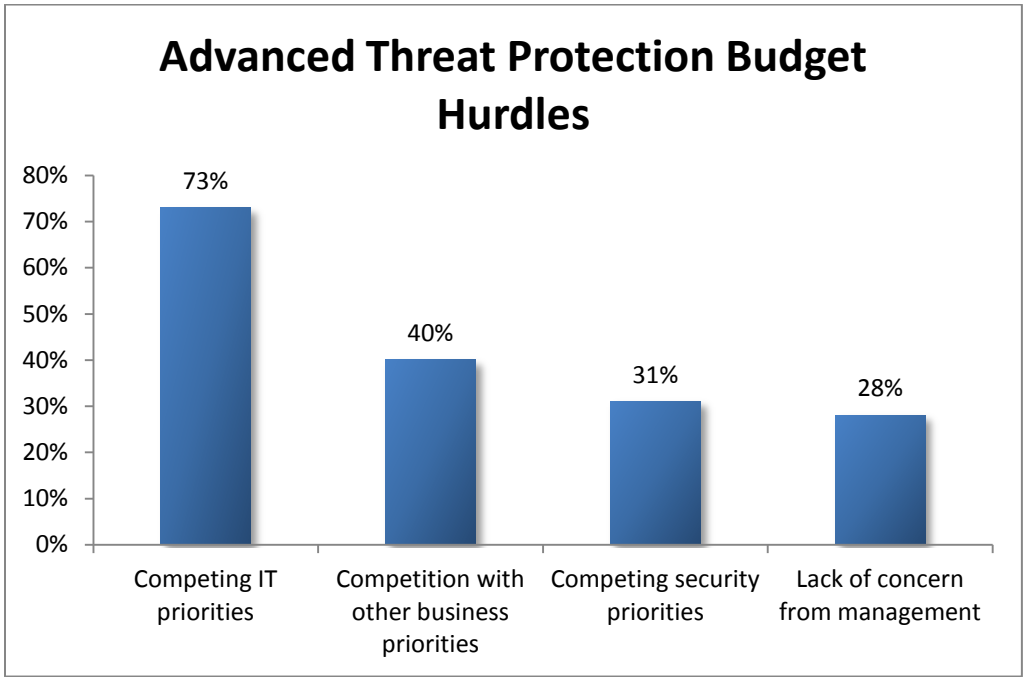

Figure 7: Challenges to Creating Advanced Threat Protection Budgets

How can security teams overcome these challenges? Figure 8 breaks down some of the common tactics security teams are using to improve budgets in their organizations:

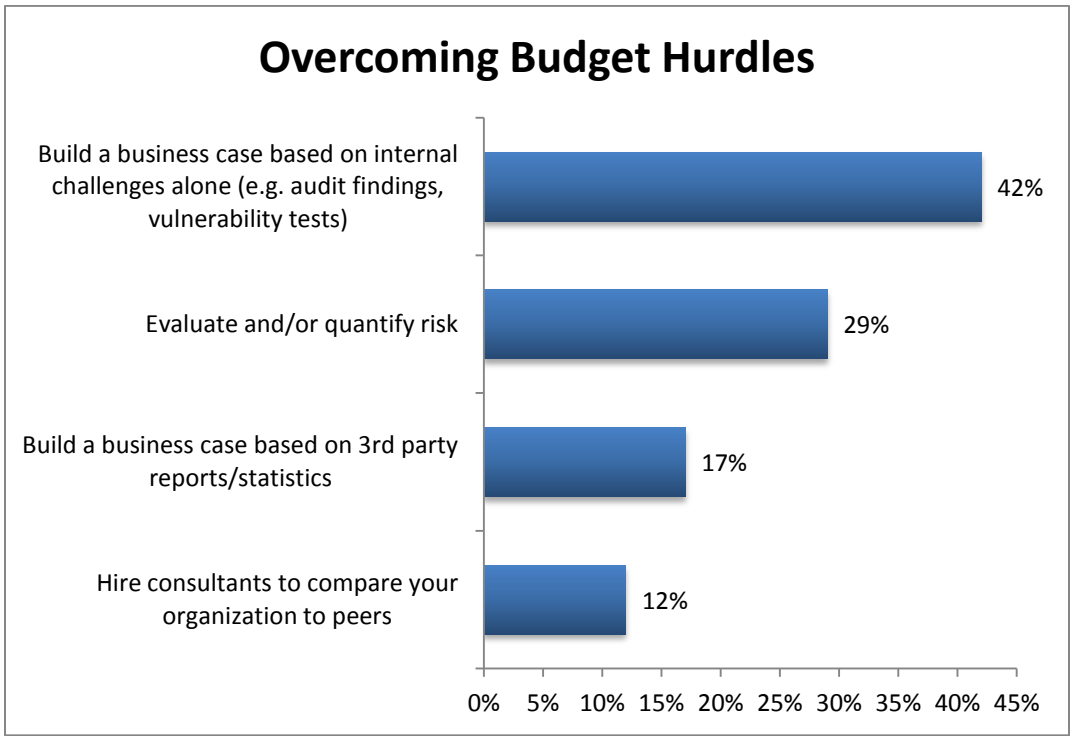

Figure 8: Overcoming Security Budget Hurdles

The majority of organizations are overcoming budget hurdles by leveraging the results of audits and penetration tests and highlighting gaps and vulnerabilities in their IT infrastructure. Risk assessment and quantification is also common, with 29% of respondents indicating this as their primary method for overcoming budget challenges. 3rd-party reports and consulting engagements focused on peer benchmarking are not as common, but still effective for some.

How is the dynamic attack landscape of today reflected in budget focus and spending for security teams? Overall, as we've seen in other survey responses, the biggest change is an increase in security spending in general (54% indicated this trend). 36% of respondents have seen some increase in spending on advanced threat detection specifically, with 32% also noting an increase in endpoint security. Only a small number of organizations are seeing decreased budgets or outsourced incident response costs consuming budgets, and several are seeing no real changes (4%), shown in Figure 9:

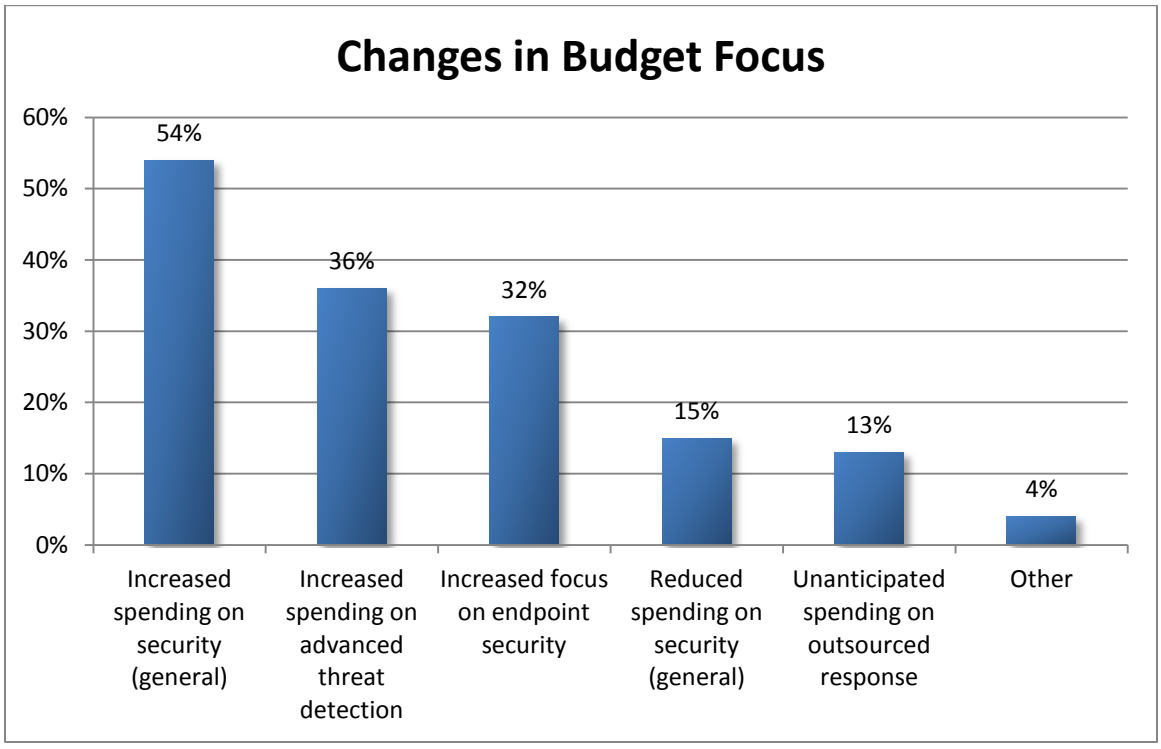

Figure 9: Changes in IT Security Budget Focus

Looking Forward

As the threat landscape changes, information security teams aim to improve their security capabilities in many different areas. What are the top IT security priorities over the next 15 months? The top priority is improving network security, followed by compliance efforts. Almost half of the respondents indicated a focus on advanced threat detection and prevention, with nearly a third noting a focus on fraud prevention and improved endpoint security, as shown in Figure 10:

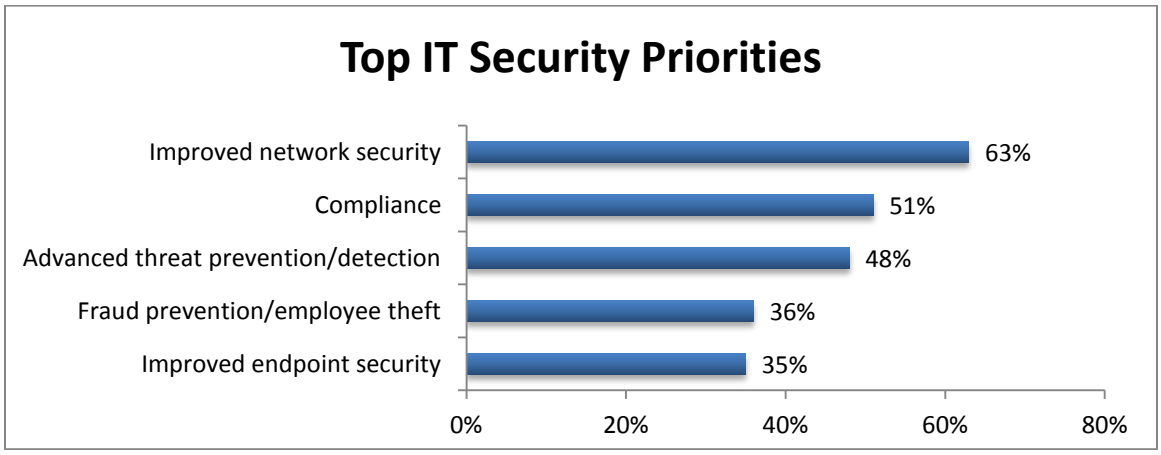

Figure 10: IT Security Priorities Over the Next 15 Months

Given these priorities, what concerns are driving business decision makers to allocate budget to information security? Not surprisingly, the majority of organizations are focused on threats from criminal actors (roughly two-thirds of responses). Some are also prioritizing spending based on improved savings from some security solutions, followed by threats from nation-state actors and competitors. Organizational growth was reported as less of a factor for organizations, as shown in Figure 11:

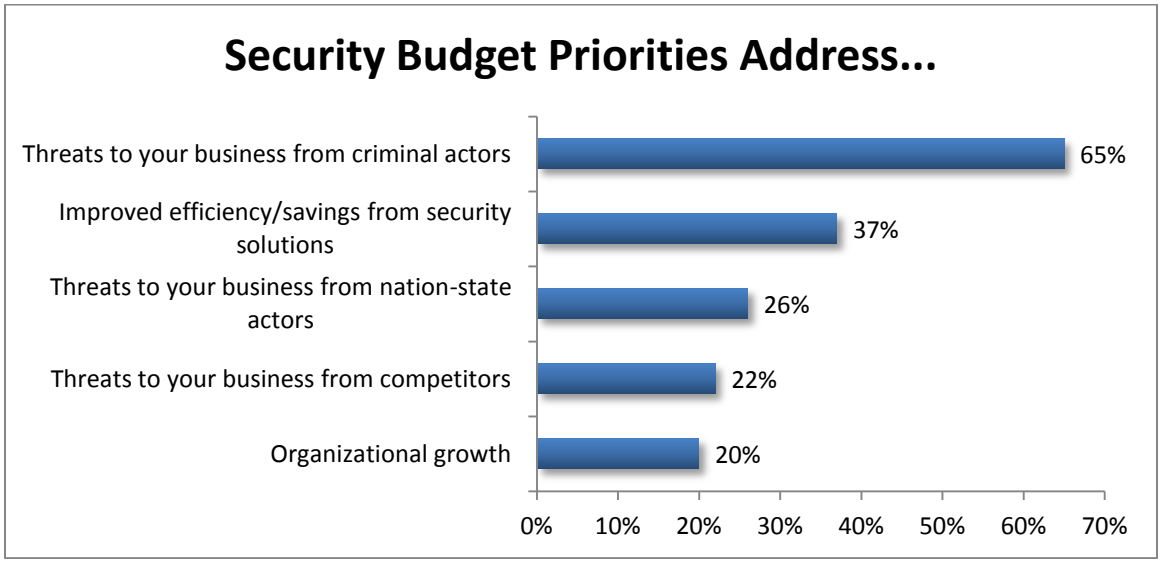

Figure 11: Security Budget Prioritization

In conclusion, what will the information security landscape look like in the near future, and how will organizations address more advanced threats and targeted attacks? Given the growing ease of compromise illustrated in the Verizon and Mandiant reports, it's likely that determined attackers will continue to compromise our networks with advanced malware. These threats, primarily from criminal actors, are steadily driving security budget priorities. Over a third of survey respondents indicated that they had experienced a data breach, and improving network security, compliance, and advanced threat protection top the list of areas in which to improve. Some notable highlights from the survey include:

- Most breaches today involve sophisticated adversaries and malware, with the primary effects of the breach including data loss, remediation costs, and some business impact.
- Most organizations are worried about criminal actors, with an emphasis on fraud and financial compromise.
- Most information security budgets are increasing, and are between 6-15% of the overall IT budget.
- Spending is increasing in a number of areas, primarily on advanced threat technology and next generation firewalls.

- IT spending priorities are the biggest challenge to improving security budgets, but security teams are making headway with risk assessments, audit findings, and threat assessments. Penetration tests are also useful.

One thing is for certain - organizations are more focused on security than ever before. With the realization that preventing and detecting breaches due to advanced threats from sophisticated adversaries is an increasingly uphill battle, there has never been a better time to focus on security spending and budgeting to improve our security architecture and controls.

About FireEye

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive "boots on the ground" — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,500 customers across 65 countries, including over 150 of the Fortune 500.

About IANS

IANS is the leading provider of in-depth security insights and decision support delivered through research, community, and consulting. Fueled by interactions among IANS Faculty and information security practitioners, IANS' experience-driven advice helps IT security, risk management, and compliance executives make better, faster technical and managerial decisions. IANS was founded in 2001 as the Institute for Applied Network Security. Inspired by the Harvard Business School experience of interactive discussions driving collective insights, IANS adapted that format to fit the needs of the information security community.