UBM Tech

THE STATE OF Cybersecurity in the Digital Economy

WIPRO Applying Thought

Balancing Accessibility with Effective Risk Management

A fast-evolving and increasingly virulent threat environment is raising the security stakes for businesses today. This, combined with the highly distributed and more open nature of today's enterprises, is testing even the best resourced corporations.

Executive Summary

To better gauge how businesses today are arming themselves against cyber threats, and to what extent trusted third-party managed security services providers (MSSPs) play a role, UBM Tech surveyed 146 business technology managers in late 2013 about the solutions they are employing to mitigate their risks.

Survey participants represent a cross-section of industries, including banking, financial services and insurance; healthcare; retail and consumer packaged goods; and energy and utilities. Respondents hold a range of management roles, from CEO and CIO to directors and line-of-business managers. The majority work for enterprises that employ 1,000 or more people. More than half of the participants work for companies with annual revenue of $1 billion or greater.

The research shows businesses battling a wide range of cyber threats, with viruses, malware and botnet-launched attacks highest on their list of concerns. New business collaboration tools such as social media, and IT delivery models such as cloud and mobility, are adding to the security challenge by introducing potential exposure points for corporate data. Businesses must rethink policies around safe use and their practices for protecting valuable and sensitive information from possible leaks.

Security spending has significantly increased as security has shifted from being a nonfunctional requirement to a business requirement. Business and technology innovations leading to the Internet of Everything and consumerization have brought security into focus.

In fact, 83 percent of businesses surveyed by UBM Tech plan to increase their security budgets in the next few years. Credit the constant barrage of threats against vital corporate assets and consumer data and the high-profile breaches of 2013 and 2014, including those at Target, Neiman Marcus and Michaels Stores, for driving enterprises to tighten security controls and operations. A detailed analysis of these breaches has brought process weakness into the foreground, along with the need for defense-in-depth security controls.

This appreciation for the critical nature of security controls and enforcements is applicable across almost

every industry. Traditional targets such as financial, retail and healthcare companies have evolved and are showing maturity in their security strategies, while newer targets, including manufacturing, utilities, electronics and natural resources, are under high alert because of "hactivism" and terrorist activities. Hackers are perpetrating intelligent attacks, morphing threat agents and initiating stealth attacks that take advantage of weak controls and process gaps to slip past corporate controls.

Organizations in all sectors are introducing new systems and technologies into their security landscape, including BYOD.

Adding to the woes of security officers are the changing regulatory requirements that make it more complex to secure the business. Key challenges include creating the required awareness and building a team of security architects and data scientists to safeguard the business with intelligence.

The Best Defense

"Defense in depth," or security at each layer spanning processes, technology, transactions and people, is what every sector is focusing on. Gone are the days where security was confined to the perimeter and point solutions. New-age businesses run using intelligence, emotions, patterns and profiles, which drives security toward convergence, analytics and posture. Asked what top security issues contributed to breaches at their enterprises, survey respondents put viruses, malware and botnet attacks at the top of their threat list (see figure 1).

Phishing and spam can also derail productivity and potentially capture personal or highly sensitive information, and two-thirds (66%) of those surveyed cited these among the top issues they face today. User error remains a major contributor to corporate insecurity, with 62 percent noting that often well-intentioned but poorly executed decisions can put critical information at risk. Weak passwords, easily hacked, can also make it easier for unauthorized users to access corporate resources.

The more extensible nature of enterprises also introduces new risks. An environment in which more external users, such as contractors, partners and guests, are able to tap into data they're not actually authorized to access can pose a major threat to the security and stability of an organization.

The Systematic Approach

So how are organizations defending their critical information in the current context of unpredictable threats while addressing changing business, technology and regulatory needs? The simple answer is that businesses are taking a systematic approach that focuses on user awareness, shredding the silos of technology and systems, as well as converging security systems for a unified view of posture and intelligence information. Organizations in all sectors are introducing new systems and technologies into their security landscape, including bring your own device (BYOD) for remote control and operational tasks; health-monitoring devices on home networks; and smart meters

Survey Methodology

In late 2013, UBM Tech conducted an online survey on behalf of Wipro on the State of Cybersecurity in the Digital Economy: Balancing Accessibility with Effective Risk Management.

A total of 146 business technology management professionals completed the survey and make up the final data set. The greatest possible margin of error for the total respondent base (N=146) is +/- 8 percentage points. UBM Tech was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

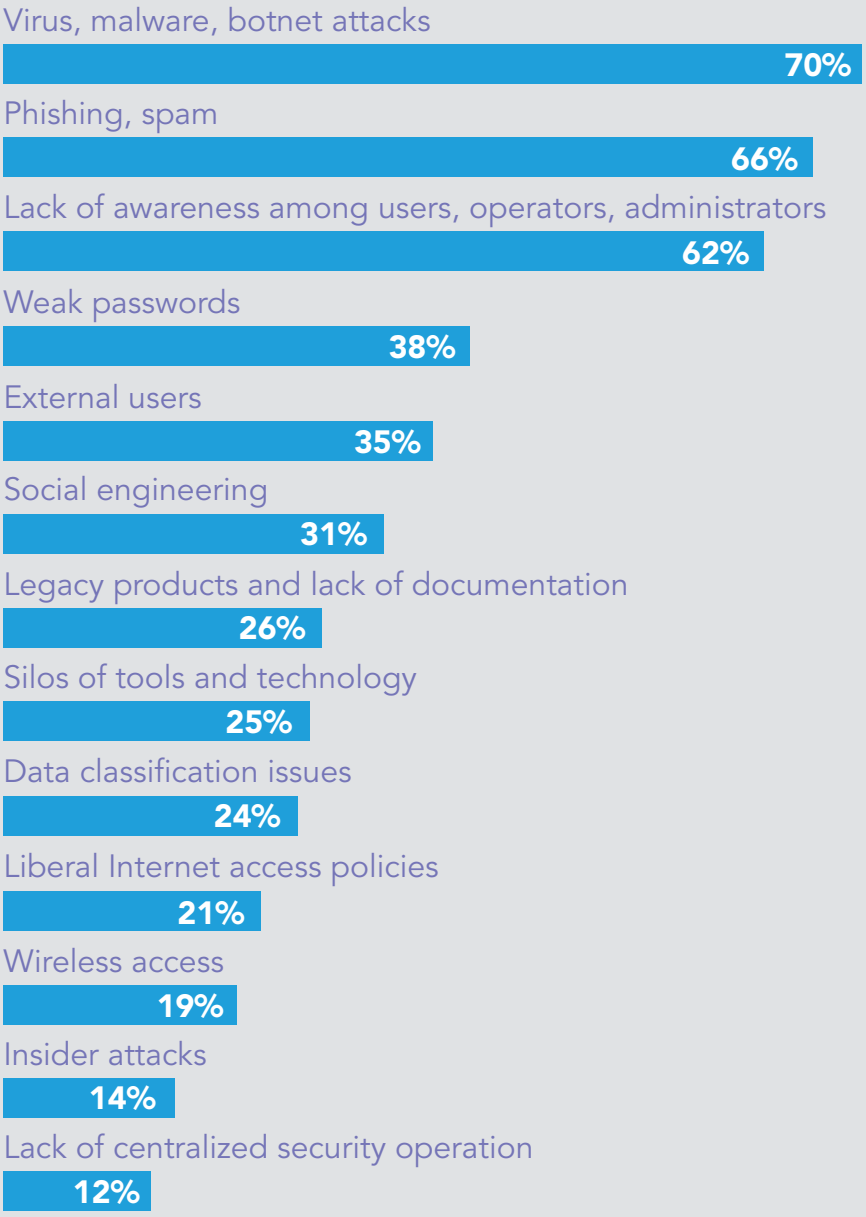
on utility networks.

In this context, 85 percent of the respondents require users to secure mobile devices with a password. Approximately three-quarters — 77 percent — engage and keep users informed by communicating information both about potential threats and about best practices with which to protect their assets.

Sixty-six percent of the respondents restrict application access to users operating corporate-owned and -managed devices. Over half — 59 percent — enable external devices based on the role of the user. So, for example, while executives may be allowed relatively unfettered access to enterprise applications, sales staff may be required to use only corporate-issued devices (see figure 2).

Businesses are also focusing on resilience and situational awareness. These steps run the gamut from requiring users to access corporate resources via a virtual private network (VPN) and USB lockdown to encrypting hard drives and using a central "gold" OS image with a predefined program for adding or limiting access. Thirty-nine percent of the participants perform security drills on a periodic basis to make sure the IT staff is prepared to mitigate the impact of an attack.

Figure 1. **Please name the top five issues that contribute to security breaches in your business.**



NOTE: Maximum of five answers allowed.
DATA: UBM Tech survey of 146 business technology managers, December 2013

A Matter of Trust

Even as companies have become more comfortable over time handing off other IT functions to third-party service providers, businesses traditionally preferred to manage the highly sensitive area of security internally. As the nature of their operations became more virtualized and distributed, and the threat environment more

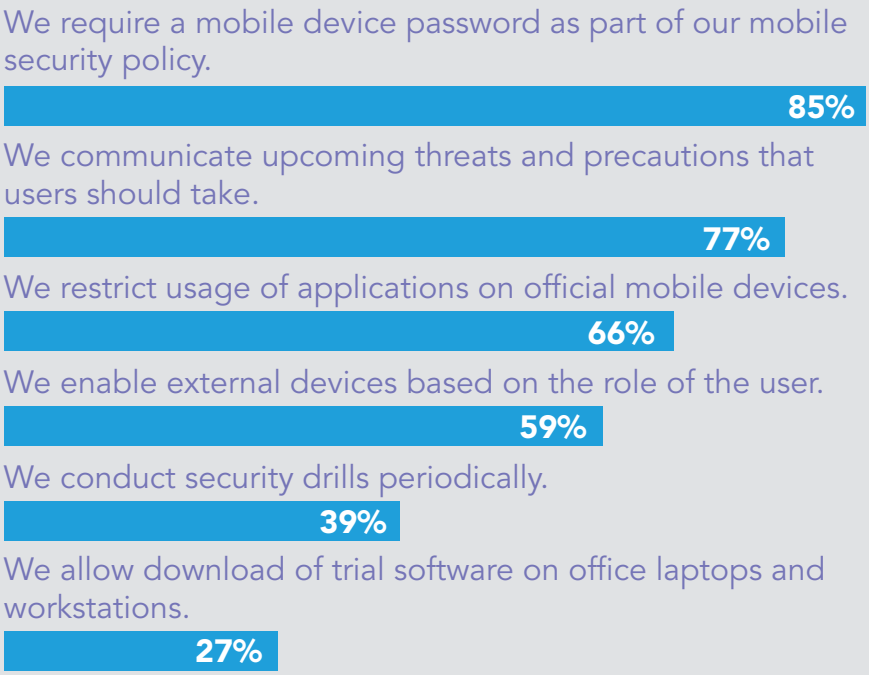
complex, enterprises reconsidered their stance on outsourcing some or all functions of IT security. With this, enterprises segregated the operational tasks from strategic programs and started outsourcing operational work to security service providers. Sixty-three percent of the respondents manage their IT and security infrastructure through service partners (see figure 3).

About 6 percent say that their provider manages more than half of their security needs. Thirty-five percent outsource less than 20 percent of their security functions to a third party. Another 9 percent handle the bulk of their IT security internally but do enlist the help of consultants for support.

So where do third parties provide the most support? There is no one specific need; instead, enterprises are looking for outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands. Enterprises turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge base (see figure 4).

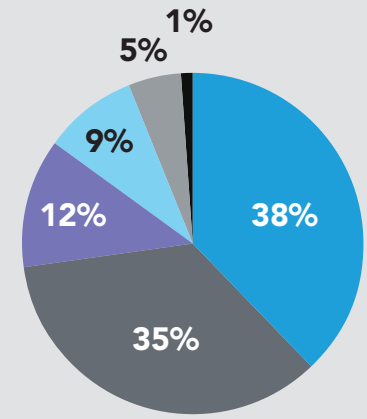
Fast evolving and still new areas

Figure 2. **Which of the following are part of security best practices in your organization?**



NOTE: maximum of five answers allowed.
DATA: UBM Tech survey of 146 business technology managers, December 2013

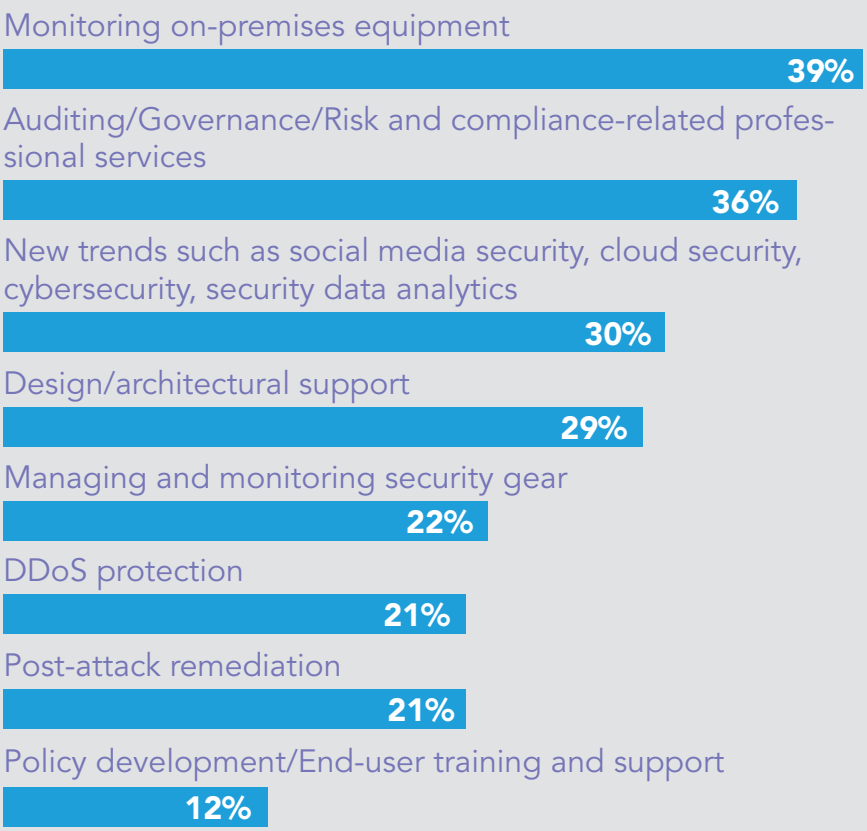
Figure 3. **Please describe your organization's overarching approach to managing security.**



- Entirely insourced/ managed by internal staff only
- Primarily managed by internal resources with fewer than 20% of security functions managed by external providers
- Mostly managed internally with less than half of security functions managed by external providers
- Mostly managed internally with the assistance of third-party consultants
- More than half of all security functions are outsourced
- Entirely outsourced

DATA: UBM Tech survey of 146 business technology managers, December 2013

Figure 4. **Which functions are you most likely to rely on a third-party managed security service provider to support?**



NOTE: Maximum of five answers allowed.
DATA: UBM Tech survey of 146 business technology managers, December 2013

such as social media top the demand list for external security support, with 30 percent relying on outside security help for issues in managing cloud, social media and cybersecurity. Twenty-nine percent seek out an MSSP for design and architecture help.

More than one-fifth of the respondents use an external provider for help mitigating distributed-denial-of-service (DDoS) attacks. Many of the third-party providers not only help with service scalability, technology expertise and tools, but they also bring intelligence and analytics to the table. They add value by letting users deploy a security solution more quickly, and by providing faster reconciliation and solution integration from an operations and resilience perspective.

Twenty percent seek out an MSSP as a reactive measure, turning to a third party to help restore services and mitigate any damage following an attack. Most businesses prefer to manage their compliance needs in-house. Just 6 percent use third parties for governance, risk and compliance management support.

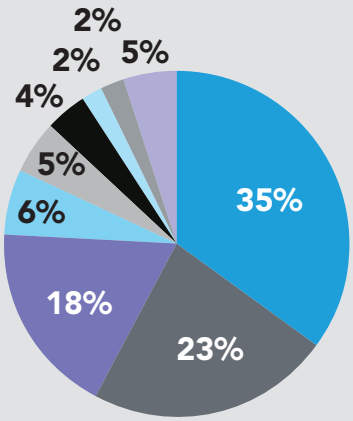
Trust and Experience Are Key

For those who do choose to use an MSSP or a security consultant, picking the right provider comes down to trust and experience. Expertise in the relevant vertical is the most widely used criterion to select the right third-party partner, but businesses also tend to choose providers with whom they already have a trusted relationship, with 23 percent citing an existing trusted relationship as an important factor in engaging with an MSSP or security expert (see figure 5).

There are distinct differences by industries in how companies factor in specific criteria when choosing a third-party provider. For example, 40 percent of healthcare companies say that an existing trusted relationship is their single most important criterion in choosing a security partner. By contrast, only 17 percent of energy and utilities consider a trusted relationship as the most important factor in their selection, instead saying that a provider's vertical expertise is far more critical.

Businesses recognize the criticality of security and compliance to

Figure 5. **What is the single most important criterion in choosing a managed security services partner?**



- Security expertise in relevant vertical segment and regulatory requirements
- Existing trusted relationship
- Deep security technology expertise
- Strong peer recommendations
- Strong skills with a particular technology
- Portal-based risk management reporting capabilities
- Analytical resources
- Proven analytical skills
- Other

DATA: UBM Tech survey of 146 business technology managers, December 2013

their longevity. And while companies are largely looking to expand their security budgets, there are still limits. Nearly half (49%) say they expect spending to increase between 5 and 15 percent in the coming years. Some enterprises are making even more dramatic increases, with 9 percent planning to raise their security budgets by more than 25 percent. Just 16 percent expect their budgets to stay flat, while only 1 percent plans to decrease security spending.

So what kinds of changes do the spending increases signify in security strategies? Going forward, enterprises are looking to simplify and improve their security operations, starting with greater standardization of the tools they use. Sixty-four percent want more commonality and heterogeneity across tools, technology and architecture. To this end, 34 percent plan to decommission legacy tools that are no longer a good fit.

One-fifth expect to outsource basic security management functions so they can focus on more strategic elements that could include areas around policy development, security architecture and data analysis. Automation will also play a key role going forward, as businesses look to remove the manual element across a number of functions, including antivirus deployment, configuration management, vulnerability management and patch management (see figure 6).

Security Drivers

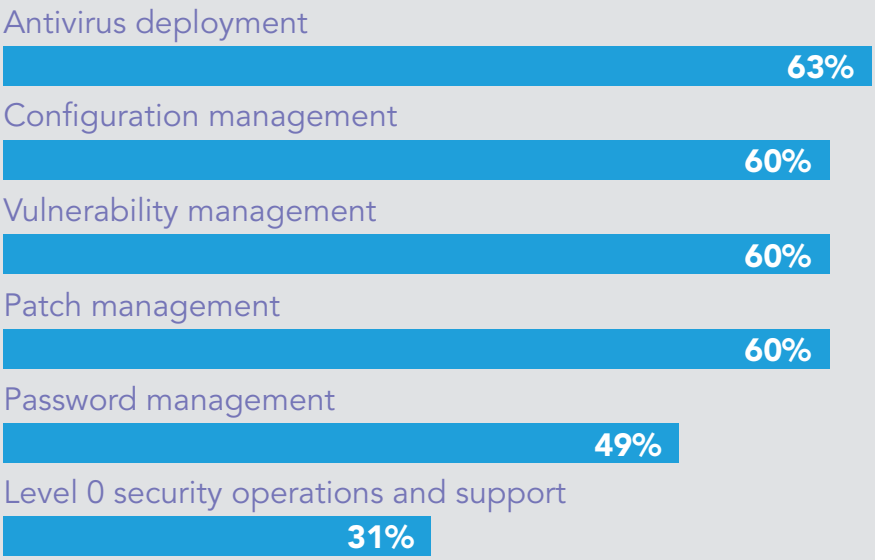
The desire to reduce human errors in order to improve the security and overall stability of the enterprise is a major driver for more automated security operations, with 44 percent of the respondents citing that as a primary reason to move away from a more manual approach to security. Nearly 30 percent say cost savings is driving their businesses down a more automated track.

Others are looking to automated solutions to free up expert staff to perform the kind of functions that require the kind of analysis, experience and insight not easily replicated by technology. Twenty-two percent want to use automation so that existing full-time employees can shift their focus to more strategic tasks.

> **The desire to reduce human errors in order to improve security and stability is a major driver for automating security operations.**

A small percentage wants to use automation as a way to supplant and maybe eventually replace internal staff. Six percent of the respondents say the main appeal of an automated solution is that it

Figure 6. **What are the top five security areas that you want to automate?**



NOTE: Maximum of five answers allowed.
DATA: UBM Tech survey of 146 business technology managers, December 2013

provides a good alternate option to using (expensive) internal security experts.

Ready for Takeoff

As attractive as automation is to most companies, businesses are more reticent about another major change in the way IT security is handled — namely, the cloud. Enterprises are making slow progress in moving to the cloud as a source for IT security services, with only 20 percent today hosting at least some of their IT security services in the cloud. Another 19 percent plan to use some type of on-demand security service within the next 12 months. However, half of the respondents say they have no intention of ever using a cloud-based security service.

There are a number of reasons behind this cautious approach to cloud-based security, not the least of which is lack of confidence in the security and stability of the delivery method and questions about the reliability and quality of service. Control, or lack thereof, is another factor, with businesses unwilling to outsource a larger portion of their security operations than they already do. Also, the relative immaturity of some of the solutions and the fact that many of the better-known options are aimed at smaller businesses with lower-scale requirements is less appealing to large enterprises. However, as more large businesses deploy cloud-based security solutions, their peers are likely to reconsider their security-as-a-service strategies.

What is clear today is that while businesses may be wary of cloud-based security, they are not only willing but eager to enlist trusted partners to fill in resource and expertise gaps to more successfully manage risk. The hope is that bringing in expert third-party partners will not only plug holes in their own capabilities but also enhance their overall security posture by providing internal staff with the tools, techniques and intelligence they need to mount a more proactive and effective defense.