White Paper

Safeguarding Vital Data Is a Battle You Can Win

intel Security

Table of Contents

There is a war going on in modern business, but you can't see it. Intruders are beating at the doors of your organization, but you can't hear them. The business world is under siege, but most businesses don't know if they've already been hit—until it's too late. Every day, customer records are lost, sensitive intellectual property compromised, and executives distracted by attacks, causing damage and fines measured in the millions of dollars. These breaches often catch businesses completely by surprise and use new approaches that can evade even seemingly strong defenses.

If you think cybersecurity is only about technology, think again. In today's always-connected, mobile, data-driven world, the increasing frequency and intensity of security breaches has made them a high-level business risk—and too many companies lack an effective response. Techniques such as malware attachments, drive-by downloads, distributed denial-of-service (DDoS) attacks, ransomware, Trojan Horse keyloggers and screen grabbers, along with social engineering such as phishing and whaling, are commonplace. And with powerful exploit kits capable of morphing attacks on the fly and cybercriminal enterprises renting access to malware services, all cybercriminals need is a credit card to wreak havoc online.

Research suggests they are proving to be extremely effective. A recent survey of Asia-Pacific businesses found that 45.5% had been impacted by a security incident during an average month[1] In another global survey, 46% of the nearly 3,000 business leaders believed there was a medium likelihood of a cybersecurity attack disrupting electrical, water, or other critical infrastructure this year. An additional 38% believed there was a high risk of such an attack.[2]

Exploding mobile and cloud usage have compounded the threat by expanding the attack surfaces companies presented to potential attackers. The emerging Internet of Things (IoT) will take this even further by building interconnected networks of data collection and processing instruments ready for exploitation by attackers.

Given these active threats to today's data-driven businesses, safeguarding vital data has emerged as one of the most significant threats to effective corporate process. Planning and executing this response has become imperative for any business—no matter what industry it operates in, how big or small it is, or how much or how little it has invested in security in the past.

There are more options than ever before to restore executive confidence as the range of security solutions available to IT managers, CSOs, and other security responders continues to expand. Whereas many businesses have stumbled along using the same signature-based detection approach, which leaves many security blind spots, an effective response combines a range of factors, including suitable technology solutions, skilled staff, adaptive design, centralized device management, and the support of qualified partners who can help extend holistic security models across Software-as-a-Service (SaaS), on-premise, hybrid, and cloud ecosystems.

Many Choices, Many Protections

Designing the right model for your information security depends on the individual structure of your business and your methods for managing security. As an overall strategic guide, however many security experts have embraced the "Five Knows of Cyber Security"[3] a five-pronged approach to structuring an effective cybersecurity response. These "five knows" include knowing the value of your data; knowing who has access to your data; knowing where your data is; knowing who is protecting your data; and knowing how well your data is protected.

Each of these steps approaches a different part of the security equation, but, taken together, they outline a framework for an effective security and governance response. These are all questions that an auditor would ask—and by thinking like an auditor, business and technology executives can ensure that they take demonstrably effective steps to safeguard vital data.

It's common knowledge that data is the lifeblood of today's business, but when asked about these questions, many business and technology executives struggle to come up with definitive strategies for safeguarding it. Indeed, many C-level executives feel completely disconnected from the security planning process. A recent survey study found that 62% of CFOs, 59% of HR executives, and 57% of chief marketing officers said they did not feel included in security planning strategies during C-suite meetings—even though these three groups oversee the most sensitive and valuable business data.[4] Even as business and technology executives juggle internal relationships in a bid to effectively revisit their security strategies, indications are that the unceasing flood of attacks and new vulnerabilities is taking its toll.

Another recent survey of security-related executives found that just 59% believed their security infrastructure is up to date and regularly updated with the best technologies available. Just 51% believe they can detect security weaknesses before they become full-blown incidents, and 45% believe they can determine the scope of a compromise and remediate it.[5]

A lack of concrete information is likely to create new problems for businesses as new legislation mandating disclosure of security breaches gradually becomes common around the world. Although 84% of respondents to a recent ISACA survey support such legislation, fully 57% said disclosure efforts would be complicated by concerns over corporate reputation; 16% said their systems weren't designed for this; 11% said it would be too expensive; and 9% were concerned they didn't have enough skills to support such a policy.[6]

Cloud Complexities

Even as companies face the increasing burden of compliance with fast-changing laws around information security, usage of cloud-based applications and services is also compounding the complexity of data-security strategies from a range of perspectives—and leaving businesses exposed as a result.

Each of these exposures relates to the "five knows." For example, data sovereignty issues—the "where" of data—were named by Asia-Pacific companies and are a key risk of adopting cloud services by 64.4% of respondents. Some 61.6% were concerned about malware outbreaks related to "who" is protecting data, while 56.2% were concerned about data theft (the "how well"), and 46.6% were concerned about human error related to who is protecting vital data.[7]

Addressing these issues is a particular challenge for today's business and technology executives because many employees are already using cloud services, unknown to and uncontrolled by systems administrators. One recent analysis found that IT administrators *believe* they have 51 cloud services in use within the organization, but that the *real number* was 730.[8]

This shadow IT presents a particular challenge for modern businesses. Even in the presence of a security policy that is tightly enforced on the traditional network, unmanaged mobile devices using shadow IT services represent a gaping security hole with direct implications on the integrity of corporate data. Despite these implications, however, companies the world over struggle to find the skills, management support, employee awareness, and budget to fix the issue.

Lack of awareness has been equally problematic in the mobile-apps sphere. A recent analysis of mobile app security found that 11% of Android apps demonstrated high-risk malware-like behaviors. Some 48.2% of iOS apps and 86.7% of Android apps demonstrated data leakage behaviors, while 62.3% of iOS apps and 86.1% of Android apps demonstrated privacy invasive behavior that affects the protection of employee data.[9]

Asserting control over such apps is crucial to safeguarding your data in a mobile and cloud context. Doing so, however, requires several key capabilities, including activity monitoring that spans on-premises, cloud-based, and hybrid environment; mobile device management (MDM) that allows for central control over employee devices being used to access corporate data and services; and data loss prevention (DLP) solutions that can monitor and manage the flow of data to those devices.

Broader use of cloud services is also driving growth in the relevance of encryption, which is increasingly used as a way of retaining control over data that is stored on public clouds or shadow IT. Encryption allows vital data to be protected at rest, in motion, and while in use—and, with tight silicon-based encryption and key management technologies built into many computers and mobile devices, its protections can flow from the business to the cloud while still being subject to centralised policy controls.

You Can't Monitor What You Can't See

The time-honored adage suggests that "if you can't measure it, you can't manage it." In the realm of data security, however, measuring isn't the biggest problem. Many businesses are still struggling to get the visibility they need to implement any kind of security controls at all.

Past security tools tended to run independently of others, generating event logs that might have considerable detail but were typically not designed to talk to other systems. With businesses often running many industry-leading DLP and other security systems, functional and integration gaps among the products created a disconnect between systems that impeded management visibility over time. Responding to threats became harder in such environments because IT security staff needed to deal with many different systems to identify and deal with security incidents. All the while, outside attackers were siphoning off sensitive corporate data.

Security information and event management (SIEM) systems improve this by providing a more holistic view of a security environment. With increasing use of cloud systems the scope of security information and event management (SIEM) tools is being expanded to provide visibility across hybrid and cloud environments as well.

Emerging threat intelligence systems, often based in the cloud to facilitate the collaborative creation of a global collective memory of sorts, pore over massive volumes of security logs to pick out behavioral anomalies that might otherwise have been missed in the flood of security data.

The need to consolidate data from many different systems—and then to deliver a comprehensive and meaningful analysis of that data—has reinforced the importance of partnering with a security vendor that is capable of facilitating the use of open ecosystems. These emerging ecosystems are built on the open exchange of new threat information, which uses open standards to collect and index details of new attacks in near real time.

Due to the high volume of information they are collecting and analyzing, increasingly intelligent security systems are also getting better at reducing the incidence of false positives, which can drain a company's limited resources for security response, allowing specialists to focus more closely on the most significant security issues.

Bringing It All Together

Businesses face a big challenge in revisiting the security technologies and practices of the past. However, given the rate business and supporting technology are moving, there is no choice but to adapt and face this challenge.

Technology strategies are a major part of the equation. New security platforms, refreshed on a continuous basis by threat intelligence platforms that harvest security information from around the world, offer the best chance possible of keeping up with the ever-changing threats posed by today's cybercriminals.

Yet for any security strategy to be successful, it is also critical for business and technology executives to look beyond the technology and consider just what they want to monitor and how. Knowing everything about your business data can be surprisingly difficult—but once it is clear what you are trying to protect and why, safeguarding your data is much easier to do.

Struggling to find enough skilled security practitioners to manage the transition smoothly and effectively? Don't worry. There are are many capable consulting practitioners in the market—many of them working with vendors—who offer deep and broad technology knowledge to help you through the process.

Ultimately, effectively protecting your data is about developing a comprehensive data protection strategy that works for the whole organization. In today's climate, that means developing data management and protection policies that reach from the core of the business out to mobile devices, the cloud, and beyond. By unifying security practices and formalizing your security response, you'll be ready for whatever security challenges the world sends your way.

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. **www.intelsecurity.com**. Intel Security is a division of Intel.

1. Telstra 2016 cyber security report—**https://www.telstra.com.au/business-enterprise/campaigns/cyber-security-report**
2. **http://www.isaca.org/cyber/Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt_Eng_0116.pdf**
3. Telstra 2016 cyber security report—**https://www.telstra.com.au/business-enterprise/campaigns/cyber-security-report**
4. IBM C Suite Study: Securing the C Suite
5. Cisco 2016 Annual Security Report **http://www.isaca.org/cyber/Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt_Eng_0116.pdf**
6. **http://www.isaca.org/cyber/Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt_Eng_0116.pdf**
7. Telstra 2016 cyber security report—**https://www.telstra.com.au/business-enterprise/campaigns/cyber-security-report**
8. **http://blogs.cisco.com/cloud/shadow-it-and-the-cio-dilemma**
9. Ibid.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com