The PULSE of IT

"Insights for forward-thinking small and midsized business leaders"

PROACTIVE ADOPTER SERIES:

Embracing foundational benefits of IT security

In a world where small and midsize businesses (SMBs) are constantly looking for ways to cost-effectively increase productivity and improve customer relations, technology takes center stage. When an organization finds a way to leverage cutting-edge technology (such as big data, mobility, and the cloud) quickly and effectively, it has the unique ability to establish competitive advantage over its peers and compete with larger organizations.

However, implementing today's new digital technologies can give rise to a host of new issues. Organizations need to be sure they have both the security technology and skills in place to prevent, handle, and combat both the known and unforeseen complications of shifting to mobile and cloud models in an app-centric world. Of course, selecting the right tools and building the knowledge base often requires engaging with strategic partners and providers capable of navigating this increasingly complex environment.

"We see IT security solutions at the heart of new technology implementation."

IT DECISION-MAKER, TELECOMMUNICATIONS, APJWC

In a recent Hewlett Packard Enterprise (HPE) survey, conducted by Coleman Parkes, of 1,500 SMB decision-makers, when asked which technology is fundamental in addressing business priorities, IT security noticeably rose to the top of the list.

Among the three adopter groups broken down in the survey, a few key differentiators regarding how these organizations are approaching security emerged. Basic adopters recognize the benefits associated with new tools, such as big data and mobility, and while they've begun embracing these technologies, they tend to be more reactive in nature, typically implementing new security tools or protocols after an event has forced the organization to take action. For instance, the motivation to adopt new technologies might be generated from customers who require mobile interactions, or a data breach that causes the organization to fall out of compliance with an industry regulation.

Moderate adopters tend to study what's available to learn about potential benefits, but they have yet to establish a clear business strategy and are hesitant to pull the trigger.

The proactive adopter group, in general, has effectively embraced big data, mobility, and cloud technologies, and now views security solutions as the binder that protects the network and business data in this shift. This group is strategic in its technology selection process, aligning investments with key opportunities to grow the business and maintain a competitive advantage and a sales and service advantage. They are also well-protected with IT security offerings, and security has become a key element in helping their companies address business priorities in a timely and effective manner.

PRIORITIES OF PROACTIVE ADOPTERS

1. Keeping the business up and running
2. Launching new products/services or moving into new markets
3. Investing in new technology to transform business

Security spotlight

The costs associated with the growing number of security breaches and the effectiveness of today's hackers are two major reasons why IT leaders value security. And despite the oft-held belief that enterprise organizations are a more likely target, small and midsize businesses are just as likely to fall victim to an attack. According to the Ponemon Institute, "The most costly cyber crimes are those caused by malicious insiders, denial of services [DoS], and web-based attacks."[1]

Mitigating these attacks requires enabling state-of-the-art IT security technologies, and implementing this level of security requires more strategy than simply installing software. At the same time, companies find themselves even more exposed as they move to digital means of enabling workplace productivity and improving customer interactions and experiences. Strategy, skills, and solid partnerships play an instrumental role in realizing success.

For small and midsize businesses in particular, the cost of failing to properly invest in IT security can be significant, with potentially damaging consequences. For example, security breaches often lead to costly, unplanned downtime, resulting in lost revenue. According to the Ponemon study, business disruption represents the highest external cost, followed by the costs associated with information loss. Specifically, "business disruption accounts for 39 percent of total external costs, which include costs associated with business process failures and lost employee productivity."

The longer a business is nonfunctional, the more it loses—yet it still has to pay the bills. In addition, security breaches tend to draw undesirable attention, including bad press, legal fallout, and customer loss, each of which has the ability to destroy an otherwise stable organization—not to mention threaten employees' job security.

PROACTIVE ADOPTERS

- Leading visionaries who embrace change
- Agile and innovative
- Willing to take risks to grow and stay ahead of competition

MODERATE ADOPTERS

- Implement when the business is ready
- Thoughtful and conservative with IT investments
- Address growth tactically vs. strategically

BASIC ADOPTERS

- Cautiously consider IT decisions
- Rely on guidance from service providers
- Risk averse, react to specific needs as they arise

1. "2015 Cost of Cyber Crime Study: Global," Ponemon Institute, October 2015, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

Making a difference

The true driver for investing in IT security goes beyond combating breaches. When organizations start with a strong, secure network, it paves the way for successful investments in big data, mobility, and cloud computing. Without security as a foundation, it becomes difficult to enable these other technologies.

Many of the benefits associated with today's disruptive technologies center on access to data. This is true whether you're providing remote access to customer account information from a mobile device or mining large cross sections of structured and unstructured data to make timely decisions. Without first having solid security in place, embracing any of these solutions can essentially expose a dangerous portal to the business network. Without question, data (especially customer data) is one of the most important assets an organization can possess. Organizations need to realize this value and protect it accordingly.

"Security risks hold your business back. When you rely on legacy IT security solutions that operate in silos, the resulting gaps and complexity can kill efficiency and squander resources you could be investing in your business."

IT DECISION-MAKER, FINANCIAL SERVICES, EMEA REGION

As one HPE survey respondent, an IT decision-maker in manufacturing from the Europe, Middle East, and Africa (EMEA) region, stressed, "Keeping staff and business information secure enables us to work efficiently and securely in developing new customers and products for market."

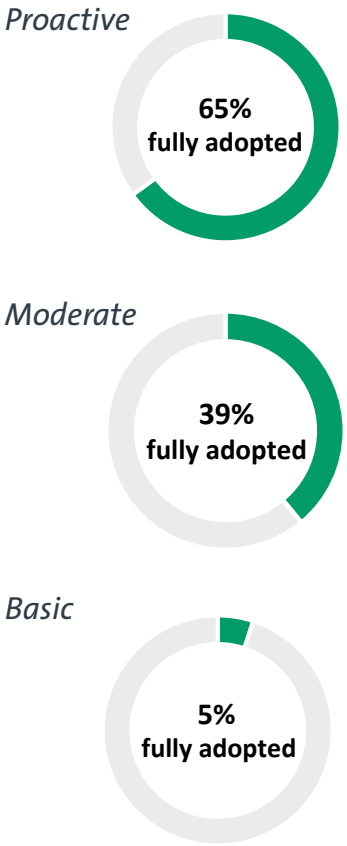
Fortunately, many firms are starting on the right path. Nearly three-quarters (73 percent) of SMBs are on the adoption path for IT security, with an additional 17 percent planning to adopt in the next 12 months. These businesses are going beyond the typical antivirus programs. Specifically, proactive adopters are taking a refined approach to ensure security is embedded in their hardware and software through the business infrastructure. These security solutions allow businesses to effectively embrace all other technologies under consideration while protecting access to valuable data.

According to the survey, the key motivators proactive adopters cited when adopting IT security solutions included the need to align IT with business units (49 percent), the desire to modernize IT (46 percent), and the need to modernize the business (46 percent).

TOP MOTIVATORS FOR ADOPTERS

- **49%** Need to align IT with business units
- **46%** Desire to modernize IT
- **46%** Need to modernize the business

IT SECURITY ADOPTION RATE



A firm's attitude toward security can make a difference in its ability to establish competitive advantage. For instance, if an organization has a proactive approach to adopting today's IT security solutions, the results can be identifiable in the company's technology investments. Those organizations on the cutting edge tend to not only recognize that each technology is crucial to the business, but they also see security as the means to shoring up IT infrastructure. One IT decision-maker in financial services from the EMEA region does a great job of putting the importance of investing in today's IT security in context, stating, "Security risks hold your business back. When you rely on legacy IT security solutions that operate in silos, the resulting gaps and complexity can kill efficiency and squander resources you could be investing in your business."

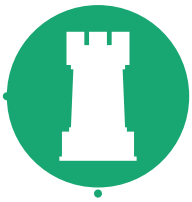
Forward-looking organizations accept and embrace the enabler role IT security can play, understanding that it's an important part of what the organization does as a business. Implementing the right set of security solutions improves business outcomes by facilitating the modernization of IT systems to improve profitability through flexibility.

When an organization embraces the traditional, reactive approach, it tends to only address security after an occurrence, such as a data breach. This can be a dangerous practice, according to the Ponemon report, especially at a time when the cost of data breaches continues to escalate. The reason for the continued climb is multipronged. First, cyber attacks are increasing both in frequency and required cost to resolve these security incidents. Second, the financial consequences of losing customers in the aftermath of a breach are having a greater impact on the cost. Third, more companies are incurring costs in their forensic and investigative activities, assessments, and crisis team management—adding to the cost of keeping the business operational, which can understandably have a negative impact on the bottom line.

When organizations remain reactionary, breaches may go undetected for months after a hacker gains entry to the business network. Even after a breach is discovered, it can take another month to mitigate the known issue. Ultimately, trying to implement security after the fact is far more expensive to effectively implement than if addressed right off the bat.

Taking action

If your organization is looking to take a more proactive stance on IT security but isn't sure where to start, here are a few steps to get you started:



STEP 1: Build a security strategy that incorporates today's technology-based challenges. With the comprehensive and seamless Internet of Things (IoT) technologies showing no signs of slowing down, mobility, big data, and cloud computing will continue to evolve. The ongoing trend to adopt disruptive technologies introduces a host of new and complex vulnerabilities into the business environment.

While big data's explosive growth comes with its own set of benefits, it also adds significant complexity to implementing IT security. Infrastructure security, data privacy, and data integrity management practices enter the picture. For instance, meaningful big data results come from leveraging disparate data sources capable of providing the most comprehensive insights into trends and anomalies. This often means reaching into various distributed frameworks. Plus, it intensifies when combined with the number of new access points added through mobility organizations.

STEP 2: Embrace a collaborative approach when crafting strategies. IT has long wanted a seat at the table when molding business strategy with digital transformation. This transformation centers on the interdependency of four key components that help SMBs thrive: mobile strategies that enable a productive workplace; cloud services for a more agile and cost-effective infrastructure; big data and analytics to act on customer and business insights in real time; and importantly, security as the foundation that protects the business throughout this transformation. Combined, these technologies impact how businesses engage customers, the speed at which they can deliver products and services, how well they innovate, and organizational reliability and resiliency. Ultimately, properly investing in technology has the ability to help solidify market position.

When IT and line of business leaders work collaboratively, there is a greater level of integration. It's not a matter of where all the minds are in the same room. For example, the sales team may go to IT when they need a solution for customer relationship management (CRM). Organizations that have already adopted a security strategy will be on the same page from the start regarding which solutions are available to them. This collaborative nature with the lines of business working as a seamless team toward a common business goal will position those organizations for success.

MANAGING MISHAPS

As with any commitment, there are potential pitfalls for SMBs as they make investments in IT security. Fortunately, with each mistake, there are proven steps organizations can take to overcome the obstacles and effectively get back on track.

"Not me" syndrome. Small and midsize businesses often mistakenly hold the belief that their organizations are not big or important enough to garner a hacker's attention. However, today's hackers are refined and actively looking for opportunities to gain access to valuable networks and data. And, the number of tools at a hacker's disposal (DoS attacks, viruses, malicious code, phishing, malware, etc.) is staggering and continues to grow in sophistication. An organization choosing to take a "not me" approach essentially puts itself in harm's way as an easy target. According to the Ponemon Institute report, although organizations in financial services and utilities and energy experience substantially higher cyber crime costs than organizations in healthcare, automotive, and agriculture, any firm can fall victim to an attack. The survey also demonstrated that small organizations incur a significantly higher per capita cost post breach than larger organizations.

Bottom line: Organizations need to realize neither size nor importance determines whether it's a target.

Going it alone. It's never the best route to make decisions alone. Being proactive requires the ability to collaborate with other lines of business to make decisions aligning with the overall business strategy. However, it's also important to seek assistance from industry leaders when making security investment decisions. A trusted partner can provide valuable insight into which technologies make the most sense for the organization, not just today, but in the months and years ahead, as well.

STEP 3: Communicate your stance on security. When organizations have a security-centric foundation, the ability to launch new products, move into a new market, and enhance customer relationships can improve. Businesses need to demonstrate to customers that their engagements benefit from integrated protection. Doing so eliminates a customer concern up front and reinforces the relationship-building process. As one IT decision-maker in the North American healthcare industry stressed, "[Embracing IT security] has helped us gain the trust of our customers. Security of information is very important."

Improving upon customer engagement is a significant priority for organizations. Customers want to know their partners are taking care of them at each and every step, and security should be step number one.

STEP 4: Learn to appreciate flexibility. While disruptive and impactful, today's technology is still maturing, as are hackers. While collaborative security strategies are instrumental in building the foundation, it's the flexibility and the willingness to shift investments when necessary that allows organizations to remain productive and protected over time.

Proactive adopters in particular understand that IT security paves the way for success in each of these other branches. IT's impact has never been more pronounced. However, without first investing in security, organizations are leaving the success of all their other technology investments to chance—an unwise gamble considering today's hackers have all businesses in their sights.