White Paper

Best Practices for Data Protection and Business Continuity in a Mobile World

A Guide for Small and Midsized Organizations

By Colm Keegan, Senior Analyst; Dan Conde, Analyst; and Leah Matuson, Research Analyst

June 2015

This ESG White Paper was commissioned by Hewlett Packard Enterprise and is distributed under license from ESG.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Introduction: The Importance of Protecting SMB IT and Business Assets

Small- to medium-sized businesses (SMBs) have a great deal to think about when it comes to ensuring their health, vitality, and success. Between a recovering economy, an increasingly competitive market environment, ever-changing market dynamics, and ongoing and persistent information security threats, SMBs need reliable and effective means to protect and secure their business data assets.

SMBs can be more agile and respond more quickly to customer demands and emerging opportunities than large enterprises, but they typically have limited financial resources to invest in IT infrastructure, and the personnel required to ensure that their businesses will keep running 24x7. In addition, customers and business partners expect SMBs to provide ready access to business information and services from any device and across any geography to improve the user experience, while employees are looking for new ways (with or without their internal IT department's blessing) to enhance their productivity.

While many SMBs are forging ahead with new initiatives like application mobility to support their customer, partner, and employee end-user ecosystems, this opens up a new set of concerns—such as whether they can safely share their business data without creating information security gaps. Likewise, how well can they protect their data across a myriad of geographically dispersed application servers and end-user devices? And to meet new business demands and be capable of capitalizing on new market opportunities to remain competitive, SMBs need their application infrastructures to be flexible and capable of growing without added complexity and high costs.

As previously stated, the fundamental challenge is that most SMBs simply can't dedicate the time or resources needed to fulfill all of their IT requirements, while also remaining focused on their core business. To overcome the challenges and risks of the digital era, while positioning their businesses for success, SMBs need to partner with professional services organizations with the expertise that can safely guide them through achieving the following six key IT business initiatives:

- **Data mobility**. With bring-your-own-device (BYOD) a common trend, businesses need to be able to create and enforce policies to enhance workforce productivity, while keeping business-sensitive data secure.
- **A strong information security framework (for external and internal threats).** Protecting sensitive and business-critical data is essential for any business. Whether the threats originate outside the corporate firewall, or internally, if company data is compromised, there is the risk of lost revenue, lost customer confidence, and loss of reputation among customers and the public.
- **24x7 application availability**. SMBs need to ensure that business applications are highly available and accessible on a 24x7 basis. With business being conducted anywhere, at any time, organizations need to provide continuous, reliable, and secure application access to their workforces, customers, and prospects.
- **Scalable infrastructure**. To grow an organization, you need to keep pace with the constantly changing needs of the business. To do this, the organization must have an infrastructure that is capable of scaling—to limit CapEx and OpEx costs, reduce time and resources expended, and deliver a consistent and productive end-user experience.
- **Pervasive, end-to-end data protection.** Data needs to be actively protected everywhere: in centralized data centers, in remote office locations, and on end-user devices in the field. In order to simplify operational management, a common backup and recovery framework needs to be leveraged.
- **End-to-end professional services.** SMB organizations need to develop key partnerships with organizations that can provide consulting, training services, and ongoing maintenance. Services can also include an array of financial services offerings, which enable an SMB to acquire the essential assets it requires to move the business forward.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

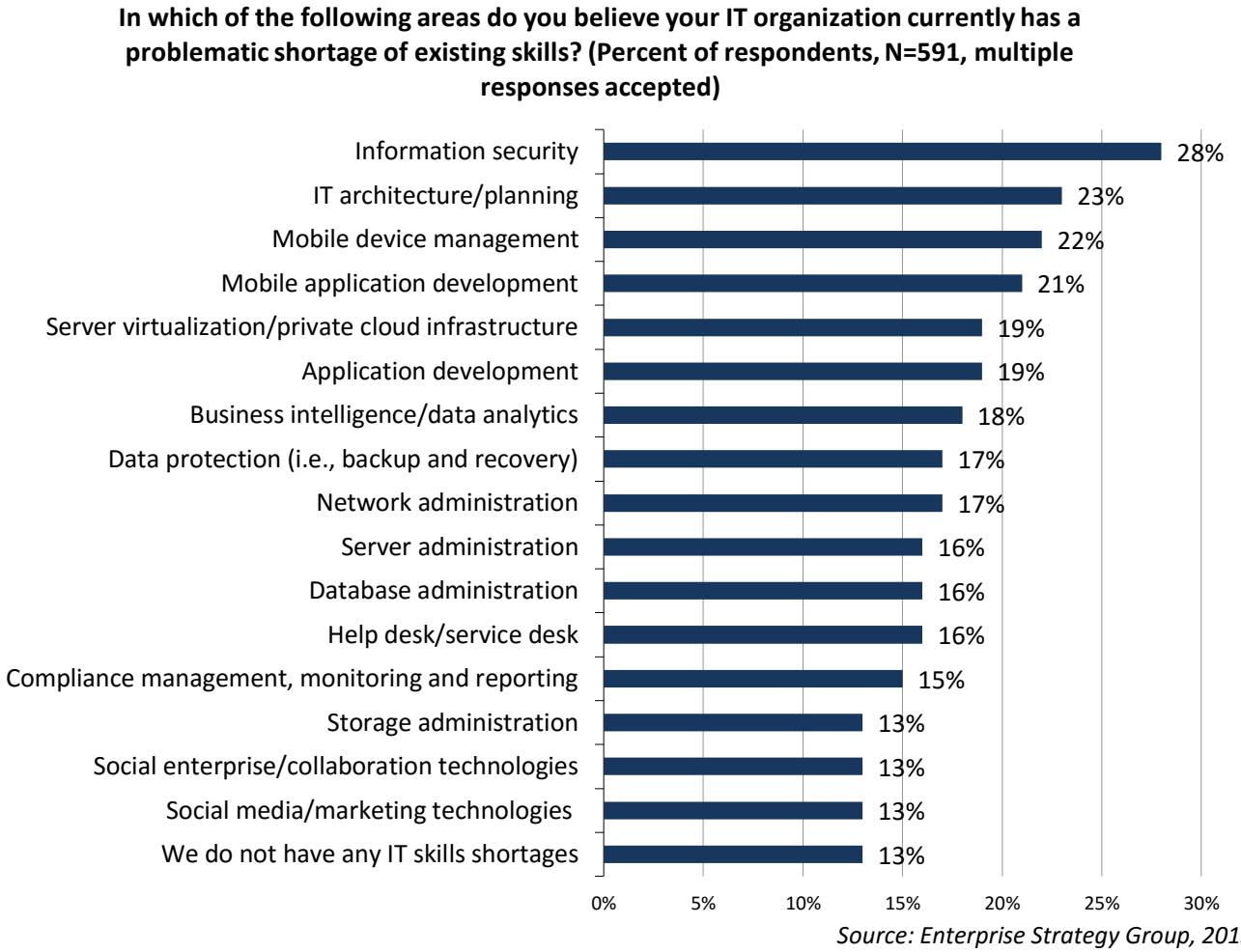
SMBs Face a Critical Shortage of IT Skill Sets

Most organizations lack many of the IT skill sets necessary to fulfill essential business requirements. In fact, according to ESG research, when responding IT professionals were asked to identify the most problematic IT labor shortages in their organizations, the most common response once again—for the fourth consecutive year—was information security (see Figure 1).[1]

The lack of security skill sets within SMBs could leave these organizations vulnerable to data hacking and theft events (both internally and externally), threatening business application and information availability, or worse. Moreover, some organizations also lack essential skill sets in IT architecture design, mobile device management, and mobile application deployment. These latter skill sets are becoming increasingly important as businesses look for ways to enhance their end-user and client experiences and tap into new market opportunities.

Essentially, SMBs need to take a holistic approach when considering how to best layer in the necessary capabilities to promote growth and ensure security in their IT environments. Accomplishing this requires the right mix of intelligent hardware and software technologies. It is also critically important to partner with organizations that can provide the professional services and expertise required to lay the foundation for a high performing, highly available, scalable, and secure infrastructure with end-to-end data protection capabilities. Lastly, through partner-provided professional training and certification programs, SMBs can build the internal expertise required to become more self-sufficient.

Figure 1. Areas of Technology with Problematic Skill Shortages



Source: Enterprise Strategy Group, 2015.

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Workplace Mobility/Bring-your-own-device (BYOD) Trend Brings Opportunities and Risks

The workplace mobility movement is zooming along the technology highway at breakneck speeds. With a wide variety of mobile computing devices (laptops, thin clients, tablets, and smartphones), and numerous file sharing and collaboration tools, business can be conducted anytime, anywhere, and on any device.

To be competitive, SMBs must provide the means for their workforces, partners, and customers to securely access the appropriate data. While this trend provides the opportunity to enhance workforce productivity, and the customer experience, it can introduce huge data security gaps and information protection risks.

Protecting Data from Outside (and Inside) the Firewall

With stories of high profile data breaches filling the news on a regular basis, most organizations are well aware of what can happen when data is not adequately protected—critical and sensitive information has been compromised leading to loss of reputation, loss of customer confidence, and loss of revenue. But these kinds of breaches, and their aftereffects, are not limited to global enterprises. On the contrary, SMBs must be just as diligent when it comes to protecting their data and their networks.

In addition, it is not enough for SMBs to only protect themselves from threats originating outside the organization's firewall; they must also be vigilant in protecting the business from threats *within* the organization. Certain employees with privileged accounts may have access to sensitive and business-critical information, financial records, and intellectual property. And those who don't have the proper credentials might try to find a way to use privileged account credentials to help themselves to an organization's proprietary data. It should not be surprising, then, that one of the top priorities for any organization is protecting the business and securing its data.

To make the situation even more challenging for IT, rather than using company-sanctioned file sharing programs, employees may use public cloud file sync and share applications to store and retrieve sensitive or business-critical information. In doing so, they could be compromising the organization's data, leaving the door wide open for malicious attacks.

So, with the trend of doing business anytime, anywhere, on any device, it is imperative that SMBs create, adopt, and enforce policies to protect business-critical and vital data—while also running the business, containing costs, and retaining and attracting customers. While it may appear to be a daunting task, it doesn't have to be.

Mobility and Information Security

SMBs need ways to enhance user productivity and make it easier for partners and customers to do business with them. And application mobility is a key business initiative that SMBs must embrace to increase their competitiveness and to open up new avenues for revenue growth. The challenge for IT, however, is that as more devices are connecting through the organization's network, there is a correspondingly higher probability of unauthorized access to sensitive business data. This data could be in the form of customer credit card numbers, bank account information, payroll files, and intellectual property. Furthermore, SMBs must be alert to the fact that data theft can occur internally within an organization just as easily as it can occur externally, from a hacker outside the firewall gaining access to the organization's network.

According to recent ESG research, 29% of responding IT professionals indicated their organizations had experienced several data breaches as the result of a compromised mobile device with another 18% indicating they had experienced at least one such event (see Figure 2).[2]

In order to help safeguard business data, SMBs need solutions that incorporate multiple layers of security. This includes:

1. **Network security:** Using intelligent network devices that act as the first line of defense in real time. Network devices first quarantine all users until their authorization is verified, and can then authorize access to certain data.

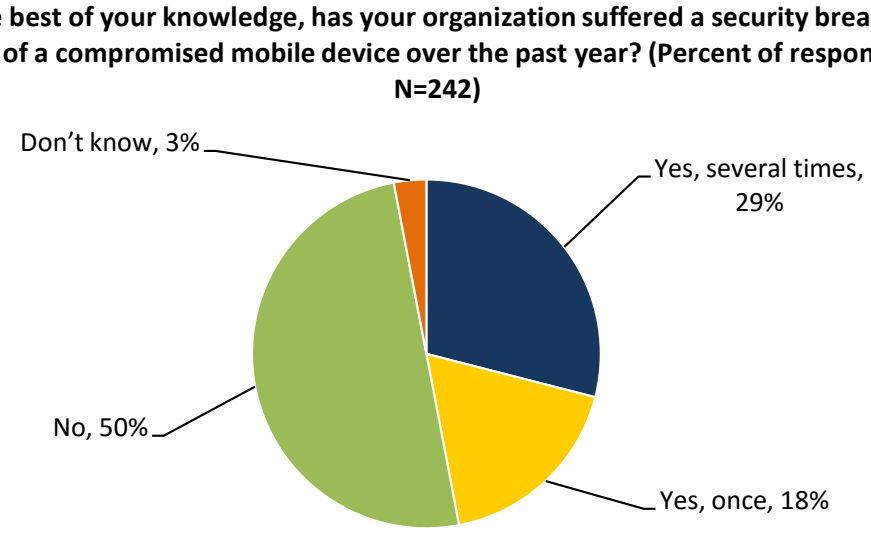
[2] Source: ESG Research Report, *The State of Mobile Computing Security*, February 2014.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

2. **Software-defined networking (SDN):** Automated end-to-end security across networking switches, routers, and wireless access points for protection against botnets, malware, and spyware sites. SDN can prioritize network traffic, i.e., business-critical vs. social media, to ensure that critical data has the highest network resource priority. SDN has the ability to isolate and inspect individual devices to ensure that only authorized users can access sensitive business applications and data.
3. **Security analytics:** Non-intrusive virtual network probes can analyze data as it is going over the wire. These probes compare traffic patterns to known normal traffic activity and flag/isolate network traffic when there is abnormal activity, e.g., distributed denial-of-service (DDoS) attacks, etc.
4. **Multi-factor authentication (MFA):** Application software that can detect when a user sign-on request is coming from an unknown device or an unknown location (foreign country). By requiring a user to key in an additional passcode that is issued to the user's known e-mail account, MFA can reduce data theft events.

The bottom line is to know who you're talking to, and know what privileges are appropriate for each user *before* granting access to sensitive business applications. "Trust, but verify" is a key strategy, and having the right security infrastructure in place is critical.

Figure 2. Have Organizations Experienced a Security Breach as a Result of Compromised Mobile Device?



Source: Enterprise Strategy Group, 2015.

Solutions that Enable Secure Data Mobility and Remote Data Protection

It's essential for SMBs to use trusted solutions that enable secure data mobility and remote data protection while reducing operational complexity and costs, and ensuring compliance with data governance and regulatory requirements. These solutions must provide a proactive defense in securing data, applications, and systems, and should ideally include the following:

- **Network switches with built-in security intelligence**. Security features such as VLANs separate traffic on a network, and access control lists (ACLs) assign user access. These solutions provide the ability to scan and identify devices when they connect into the network, and then assign application access privileges based on the user (e.g., a guest/visitor account or an employee).
- **Automated vulnerability signature and patch updates.** As new viruses are identified, organizations will need to update their virus signature databases as soon as they are available, to reduce their window of exposure.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- **Remote wiping tools**. Because data can live anywhere and on any device in an organization, SMBs need the ability to remotely wipe a device wherever it may be. This capability protects against data theft should a device be lost or stolen.
- **Secure application authentication**. While SMBs would like to enable remote access capabilities for their workforces as well as for partners and customers, this opens up brand new security attack vectors. Mobile access points can be compromised, so it is vital for IT to use a means of secure application authentication. The BYOD trend has made it even more challenging for IT to protect corporate data, so using multifactor authentication adds another layer of protection.
- **Professional support services**. From initial design, configuration, and implementation, to ongoing support, SMBs need professional services partners that can help organizations drive increased levels of security and automation, ensuring the continual protection of the business.

The Secure Network: Laying a Strong Foundation for Business Protection

The Need for a Multilayered Approach to Securing the Business

Managing and securing the network is a critical part of any organization's IT infrastructure. The challenge for SMBs is to enable IT staff with generalist skills so they may fulfill many administrative roles such as that of a network administrator, wireless device administrator, and security administrator. The need for IT administrator simplicity is especially important given the fact that, as shown in Figure 1, ESG research has found that information security and mobile device management skills are in short supply in many organizations.

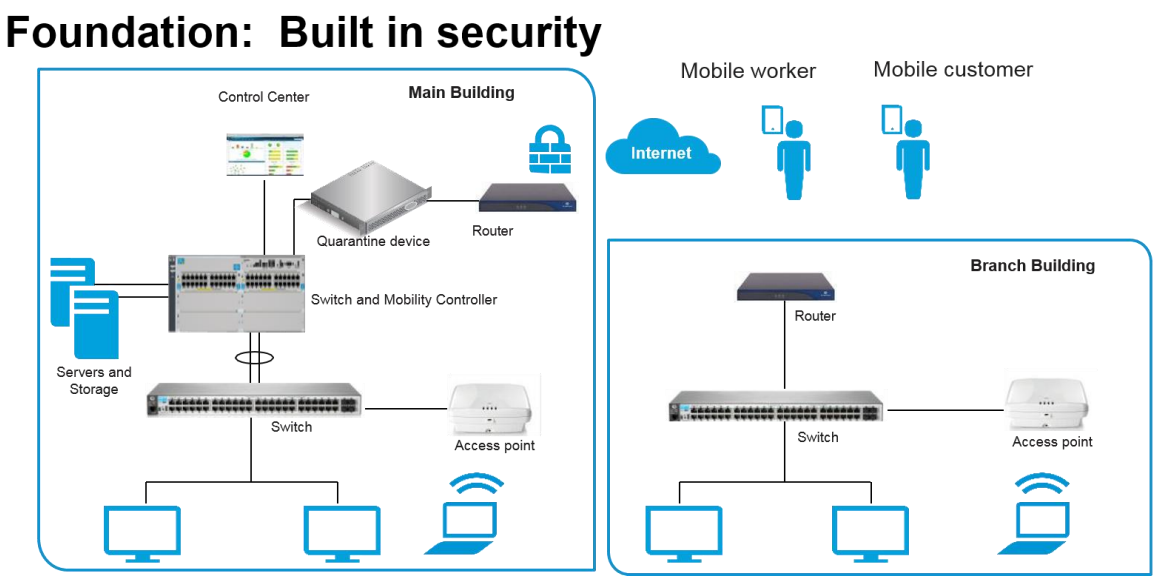
With the increased diversity of BYOD devices and pervasive use of Wi-Fi, it is no longer sufficient to rely on outdated security approaches designed for a homogeneous environment. A multilayered approach is necessary to secure the business through all phases of how a device or user connects with in-house resources to access business data. Relying solely on a strong perimeter defense may expose the business to threats if multiple entry points exist. For example, an improperly secured BYOD mobile device can introduce a potential threat through a Wi-Fi access point. More specifically, the various aspects that SMBs need to consider when implementing network security are:

- **End-user devices.** IT must be able to control the admission of end-user devices into the business network.
- **Straightforward access.** Once the device and user are admitted into the network, additional access should not be cumbersome—requiring authentication at each step is onerous and reduces productivity. Once a device is identified to the network, it should not have to repeatedly prove its identity.
- **Identification of end-users.** Users must be identified as they navigate through the network. Accessing resources within a network is performed with a purpose, so it must be tracked.
- **Identification of threats.** Unknown access requests to key resources must be identified and quarantined.

The need to secure infrastructure, devices, and information assets, whether associated with mobile workers, located at remote and branch office locations, or located within the corporate network itself, is represented in Figure 3.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 3. Security Must be Applied at All Layers of the Network



Source: Hewlett Packard Enterprise, 2015.

There are other considerations that SMBs must take into account when developing a multilayered security strategy. First, there is the role of employee training. For example, employees must be trained to follow essential security best practices such as password-protecting their laptops, using strong passwords (and regularly changing them) when accessing business systems, and avoiding downloading programs from insecure web sites. This is a critical first line of defense in the efforts to keep the business secure.

Second, SMBs do not have the luxury of relying on a large team of specialists for each aspect of network security. Third-party professional services can assist in many capacities, ranging from network security assessments to infrastructure deployment and other day-to-day operational tasks. Third-party assistance can help create an integrated, multilayered solution and improve the effectiveness of an SMB's staff.

Integrating Security and Management Tools to Ensure Visibility and Protection

As businesses allow more devices to connect to their network on a daily basis, it's crucial to be able to access a unified view for network management and security policies as it's difficult for IT to manage the devices individually. Since a system is as secure as its weakest link, an overall view of the network is also required for comprehensive security. Both the hardware and the management software must be integrated to provide this end-to-end view. Having a fragmented set of management tools is not useful, and slows responsiveness by imposing repetitive tasks. Additionally, without an integrated approach, network administration becomes a bottleneck that prevents deployment of new services and applications, and may prevent the matching of events and data from different tools, increasing the potential for manually introduced errors. In fact, ESG research has shown that an integrated network security architecture is one of the most important factors for an organization's network security strategy (see Figure 4)[3].

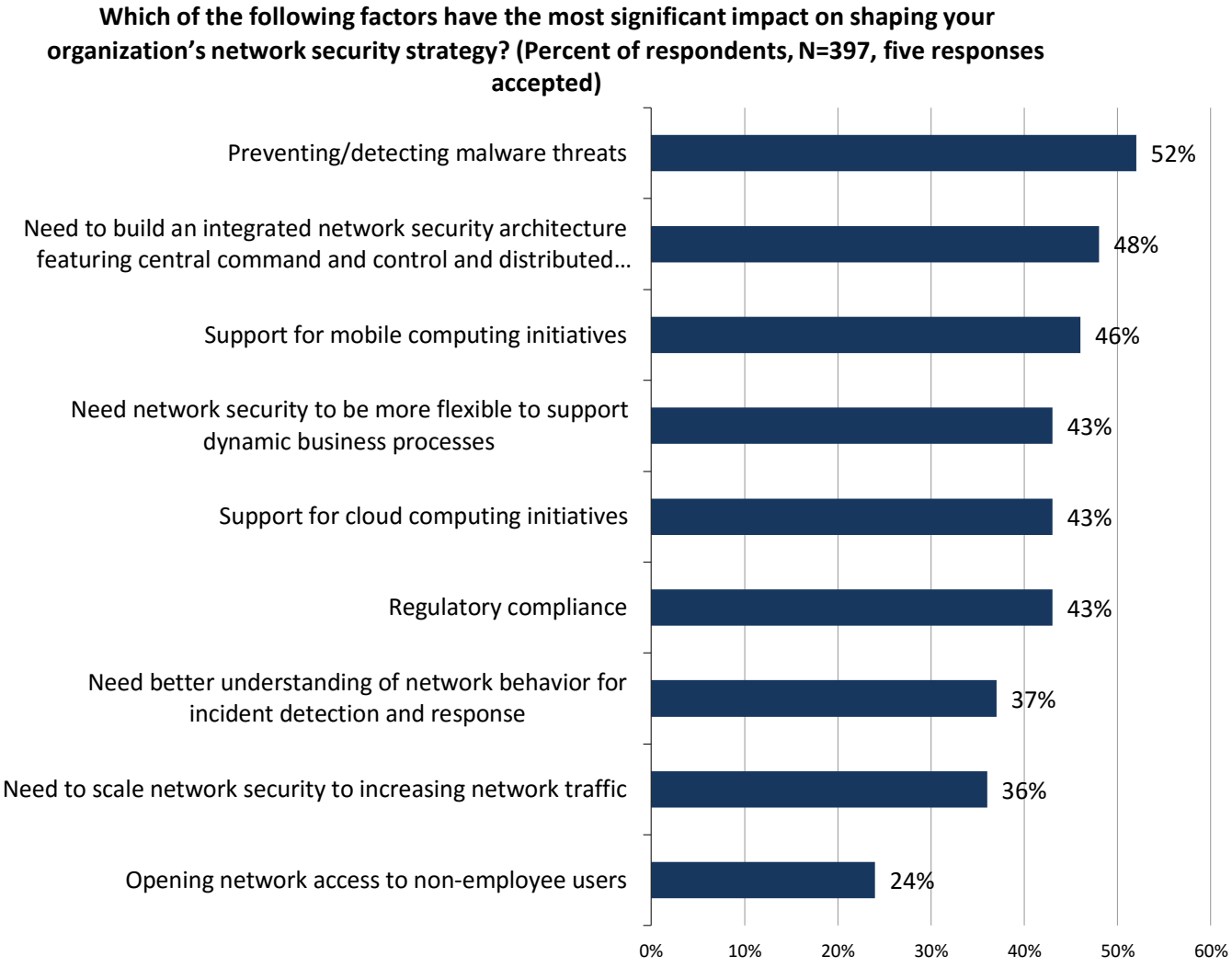
Organizations can benefit from having embedded security capabilities in their network devices. Examples of these capabilities are: VLANs for separation of network segments, ACLs for controlling traffic, and IEEE 802.1x for network authentication. If an organization has existing devices, they should look for and use these features. If evaluating new equipment, organizations should choose devices that provide, at a minimum, VLANs, ACLs, and IEEE802.1x. As previously mentioned, protection against distributed denial-of-service (DDoS) attacks, as well as multi-level access controls, are important for additional security.

[3] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Additionally, IT generalists will benefit by centrally managing the network infrastructure from an integrated management console. IT can be freed up from routine security tasks by providing the appropriate self-service management tools to end-users. This not only enables end-users to self-register their BYOD endpoint devices into the network, it also helps to reduce the time it takes to "onboard" new users.

Figure 4. Factors That Have the Most Significant Impact on Shaping Organizations' Network Security Strategy



Source: Enterprise Strategy Group, 2015.

Conformance to Industry Standards and Processes is Critical

Network devices can vary by configuration—wired or wireless (Wi-Fi), or physical or virtual (VLAN or SDN-based). Although one needs to treat each network's characteristics separately, it is important to view them in a unified manner. Organizations can no longer segregate company-owned IT assets such as company-issued laptops, from employee's BYOD devices like tablets and smartphones. Instead, IT needs to treat all device types consistently.

Tools that provide security must be easy to use, and intuitive for end-users. As new staff is onboarded or third-party professional services staff are introduced to a project, it is not efficient to start training staff on new interfaces or complex security processes. Instead, using well-known administration processes will help organizations work more efficiently. Reliance on well-known standards in technology and processes will provide familiarity and completeness in coverage so that no part of the infrastructure is neglected.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Need for Real-time Threat Protection

Security threats on the network need to be dealt with in real time, and proactively. Intruders are increasingly sophisticated and frequently change their attack methods. Consequently, threat detection systems based on exploit signatures are no longer sufficient to protect a network. In addition, malware detection needs to be based on real-time knowledge of the latest exploits. A range of malware activity such as data exfiltration, ransomware, or click fraud need to be prevented. Because SMB IT administrators cannot devote all their efforts to staying abreast of the latest low-level security details, relying on an automated infrastructure to enforce network and application system security would free them up for value-added tasks.

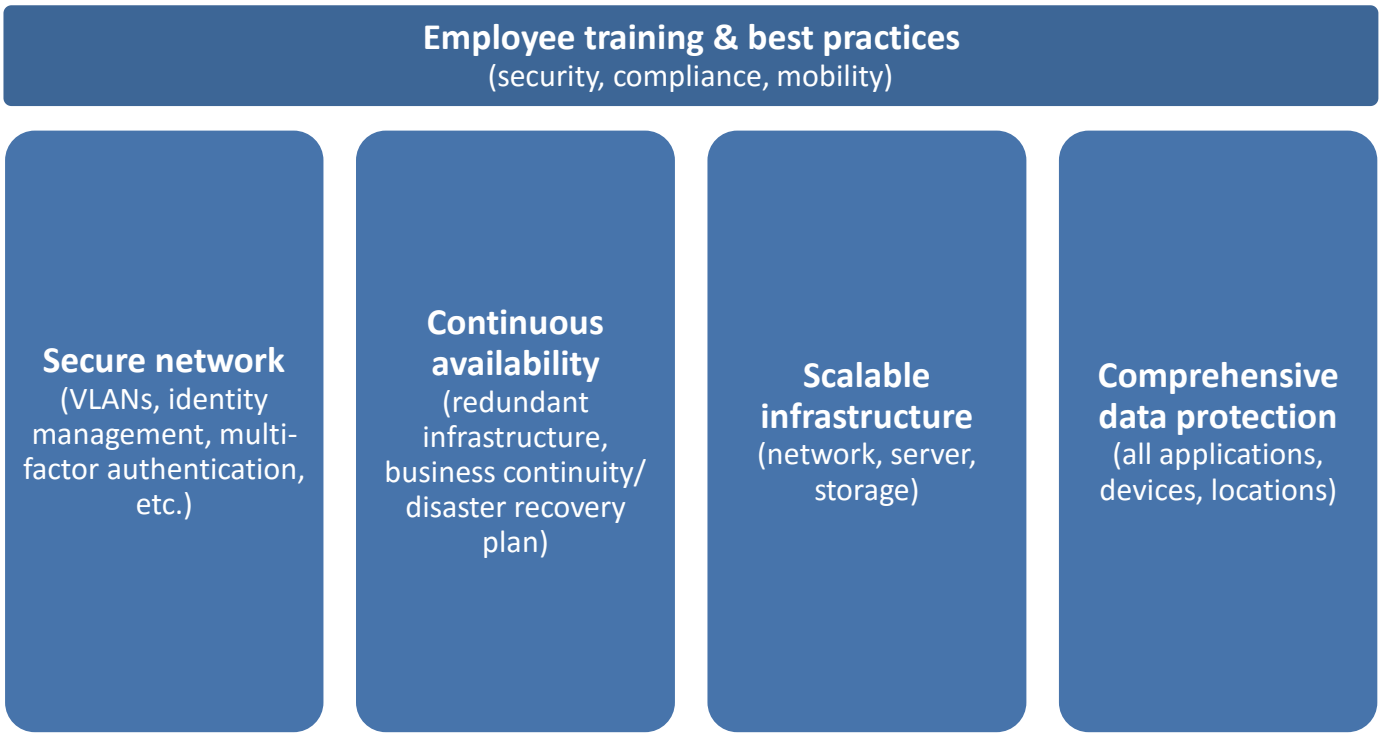
While the security threat landscape is vast and new threats are continuously emerging, businesses can erect an effective, comprehensive defense that mitigates risk without impeding business activities. The key is to select solutions which take a multi-layered, end-to-end approach to security management, and partner with services organizations that can apply these technologies to meet the unique needs of the business.

Beyond Security

But security is only the first piece in the larger IT infrastructure puzzle. To keep the business running, SMBs also need to protect data wherever it lives. This means that IT must have the ability to quickly restore data on-demand as well as scale application hardware quickly, easily, and affordably, to meet new business requirements.

As critical as a secure network is, it is just one of the components of a comprehensive IT strategy to help keep the business protected and running (see Figure 5).

Figure 5. The Pillars of SMB Business Protection



Source: Enterprise Strategy Group, 2015.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Additional IT Considerations for Protecting the Business

Continuous Availability as an Essential Competitive Tool

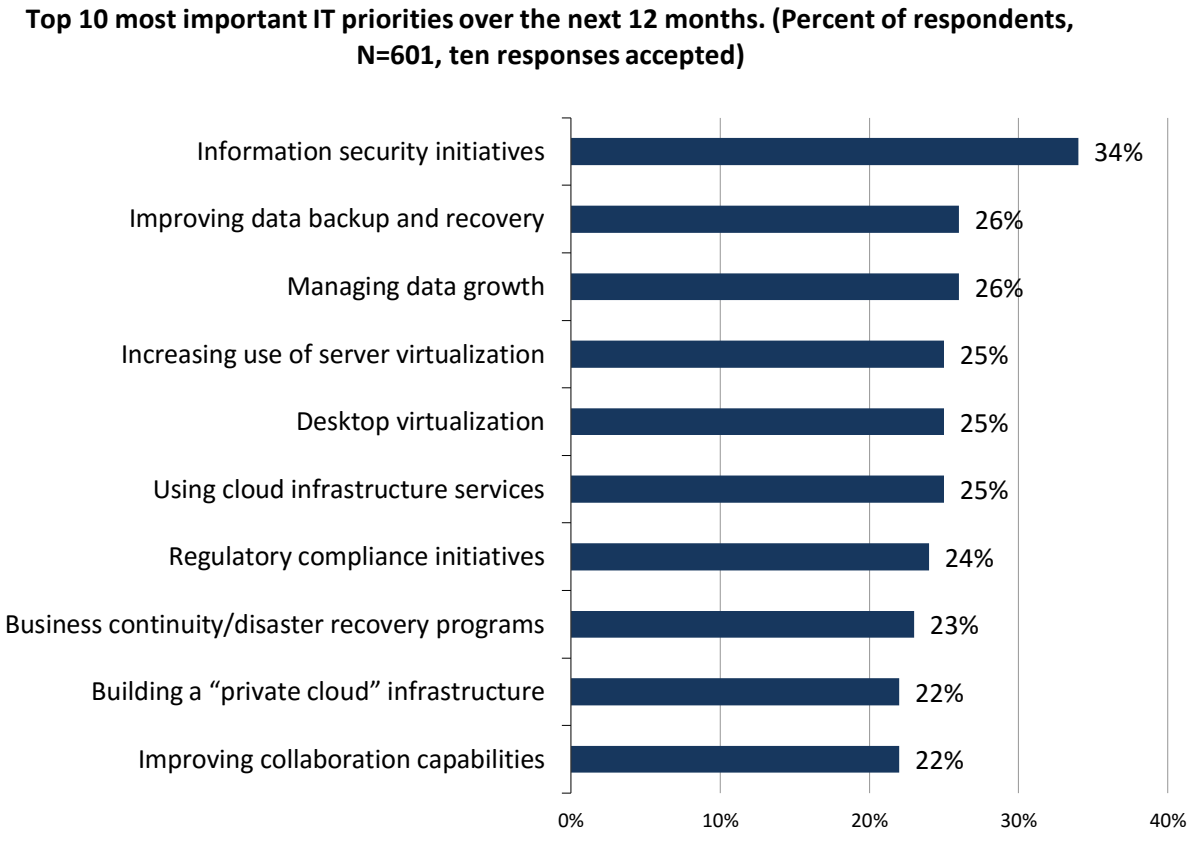
In an extremely fast-paced business environment, downtime is not an option. To be successful, an organization's business application resources need to be available continuously, 24/7. This means that critical business services need to be highly resilient and capable of withstanding a wide variety of outages. Lack of application availability, or worse, the loss of critical information, can result in the loss of revenue, decreased workforce productivity, loss of customer confidence, and irreparable damage to the company's reputation.

To mitigate the risk of application service downtime, it is essential for SMBs to take a proactive, rather than a reactive, approach. Planning is key, and preparing for "what if" scenarios is vital.

In actuality, many disasters occur as the result of everyday business system outages, such as the loss of power, the accidental deletion of data, or a database corruption, rather than a cataclysmic event like an earthquake or a tornado. It's vital for an organization's IT infrastructure to possess built-in data protection capabilities that can ensure the timely recovery of business information in the event of a data loss event resulting from human error, a hardware malfunction, or a malicious attack.

Based on recent ESG research, improving data backup and recovery ranks as one of the top IT priorities most reported by respondents, second only to information security (see Figure 6).[4]

Figure 6. Top Ten Most Important IT Priorities for 2015



Source: Enterprise Strategy Group, 2015.

To further reinforce IT infrastructure availability and information resiliency, SMBs may want to leverage data replication technology so that critical business data can be continuously copied to an alternate data center in a

[4] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

remote geographical location. Doing this can help ensure that business revenue-generating applications can be rapidly recovered in the event of a site-wide outage resulting from either a manmade (e.g., construction equipment severing a telco link) or natural disaster (e.g., flood, hurricane, etc.).

In addition, it's critical for SMBs to have a well-thought-out and fully documented disaster recovery and business continuity plan in place, complete with service run books that prescriptively detail what needs to be done to resume normal operations following an outage or disaster event. This is where professional services organizations can provide the appropriate best practices, data protection, and disaster recovery methodologies to help ensure that an SMB's IT investments in information infrastructure resiliency will pay off.

IT Infrastructure that Can Scale On-demand

To maintain business agility and stay ahead of the competition, organizations need computing resources—server, storage, and networking—that can easily scale on-demand to meet existing, as well as new, business requirements whether in virtualized or physical server infrastructure environments.

With virtualization, IT has the ability to easily spin up new applications on-demand with minimal effort, more cost-effectively, in less time, and using fewer resources than with a traditional physical infrastructure. In doing so, organizations can improve efficiencies without compromising business application performance. Benefits of virtualization also include: reduced rack space consumption, lower power and cooling costs, and far less time spent configuring and provisioning new application server resources. This flexible computing infrastructure can enable greater business agility and allow the business to scale gracefully over time.

But in order to attain the greatest possible return on their virtualized investments, SMBs need scalable computing platforms that can support higher application-to-server compute ratios. In other words, the greater the number of applications that can be supported by the underlying server platform, the greater the potential ROI, both in terms of operational and capital expenditure cost reductions. One of the keys to realizing these benefits is working with experienced services organizations that have mastered the art of architecting and implementing virtualized environments.

Unified and Centralized Data Protection Is Essential

As previously stated, ESG research continues to track data protection as a top concern for SMBs. Regardless of where information "lives," (in the data center, in remote office locations, on end-user devices, or in the cloud) it is of paramount importance for SMBs to have a simple, streamlined, and centralized way to reliably protect and manage highly distributed data.

When backup processes are complex, it can create data protection gaps and consume an inordinate amount of IT administrative time. This can leave organizations vulnerable to data loss, increase their operational costs, and deplete already limited IT resources from focusing on core business activities.

An easy-to-use, automated backup solution that is centrally managed can save IT valuable time and resources, and free up IT staff to perform more value-added activities. While an automated backup solution may make life easier and more efficient for IT, end-users also benefit. Today's workforce uses a variety of devices, including laptops, thin clients, tablets, and smartphones, which all need to be backed up on a regular basis. With automatic backup solutions running in the background, the process is transparent to the end-user, with no impact to device or application performance.

The appropriate backup solution should provide the following:

- **Ability to mitigate data loss events**. By reducing the effects of a data loss event, disruption to business or productivity is eliminated, or kept to a minimum.
- **Self-service restore capabilities**. By granting end-users the ability to generate their own file restore requests without intervention from IT, time and resources are saved. Employees can also minimize disruption to their productivity.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- **Employee data restoration following device loss/theft**. With the right backup solution, an end-user can easily restore his data on a new device without any formal training within hours as opposed to days, and with no assistance from IT.
- **Redundancy for added protection, while saving time and resources**. Incorporating the cloud as part of an effective backup solution allows IT to gain the redundancy of an off-site facility for added data protection, without committing to the time and expense of a dedicated DR environment.

End-to-end Professional Support Services

Many enterprises have large staffs comprising a variety of professionals who specialize in a number of areas. On the other hand, many SMBs have lean IT departments comprising a small number of generalists, and perhaps an expert in one particular area. This means that internal IT support is generally limited, and has limited bandwidth.

So how can SMBs stay competitive and agile, take advantage of new business opportunities, and safeguard the security of business-critical and operational data without a large dedicated staff of technology experts? The answer: third-party professional services.

From technology and support services to financial services, it's important for IT organizations to have access to a broad range of IT professionals whom they can rely on to educate, train, and assist their IT staffs. From professional services for infrastructure implementations to comprehensive and executive-class support, training/education, and financial services, SMBs can benefit.

As previously mentioned, ESG research indicates that many organizations believe they employ professionals who lack certain skills to protect and grow the business. These skill shortages range from information security to mobile device management and private cloud technologies (i.e., virtualization).[5]

Rather than do without the help of knowledgeable employees trained on modern security tools, SMBs should look to work with highly skilled and trained professionals to supplement their internal IT staffs. Third-party professional services are just what an SMB needs—not only can they show IT staff how to effectively implement and maintain their technology systems, but they can help them identify and remediate any system issues on a continuing basis.

Third-party support services can help SMBs with the following**:**

- Getting up and running faster with startup, installation, and deployment services.
- Ensuring that business-critical and operational data is protected and secured by leveraging remote monitoring and other proactive services.
- Resolving hardware and software issues quickly and more easily. This results in reduced downtime risks (loss of productivity, loss of customer confidence, loss of revenue), while improving business uptime; and enhancing customer, partner, and workforce satisfaction and productivity.
- Providing on-site support, whether the business requires support on an ongoing, per-project, as-needed, or customized basis.
- Conducting in-house training so that staff are kept current on server, storage, management, and open source-related areas, gaining essential knowledge while eliminating time away from the business.
- Offering IT capital finance programs specifically tailored to enable SMBs to stretch their purchasing power and grow their businesses.

In essence, professional services can improve the efficiency of SMBs by helping in-house workforces get things done more quickly and efficiently, enhancing their productivity, and reducing their costs.

[5] Source: Ibid.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

Organizations of all sizes must be prepared for all those things that could possibly compromise business-critical and sensitive data. But when it comes to SMBs, it's essential to take a number of factors into consideration to protect the organization. These factors comprise the overall plan for protecting data and ensuring the business will continue to run at optimum performance despite the various threats bombarding the organization day in and day out.

First and foremost, SMBs need a comprehensive plan detailing how to deal with the following:

- **Data mobility**. With BYOD a common trend in facilitating workplace productivity, as well as customer and partner satisfaction, do you have strong policies that you enforce to keep business-critical data and sensitive information safe?
- **Proactive security**. While we might hear about external hackers causing high profile data breaches, breaches can and do originate internally far more than we are aware. Knowledge is power and SMBs must have a solution in place that protects against both external and internal threats.
- **Continuous, 24/7 operation**. What systems need to be put in place so that the business will be able to continuously operate, 24/7, with minimal or no downtime? How will the business be protected and monitored, and by whom—in-house or third-party resources, or a combination?
- **Scalability**. How will the business rapidly scale both virtualized and physical IT infrastructure to continuously meet its growing needs? What systems, hardware, or software currently contribute to scalability, and what additional tools/solutions are needed?
- **End-to-end data protection**. Because data can live everywhere, it's essential to know that your data is protected, whether in centralized data centers, remote locations, or end-user devices. Simplified operational management and a common backup and recovery framework are all part of end-to-end data protection.
- **End-to-end professional services**. Because SMBs don't have the staff or bandwidth to "do it all," they must cultivate key partnerships with organizations that can provide consulting, training, and maintenance services. Additionally, using third-party financial services can keep SMBs up and running, helping to grow and move the business forward.

Hewlett Packard Enterprise's "Just Right IT" solutions provide a comprehensive set of IT infrastructure hardware and software solutions that can be uniquely customized to meet the needs of the SMB. Combined with partner-led professional and financial services offerings, SMBs can move forward on their most pressing business initiatives, such as BYOD and web mobility, to grow their businesses and stay competitive without compromising data security, information protection, or application availability. HPE's Just Right IT solutions enable SMBs to focus on revenue-generating activities rather than worrying about the structural integrity and security of their IT environments.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

HPE Document No. 4AA5-8753ENW

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com