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

White Paper

Managed Security Services–A Big Win for Small Businesses

By Christina Richmond, ESG Principal Analyst and
Kevin Rhone, Director, Channel Acceleration Practice

January 2020

This ESG White Paper was commissioned by ESET and is distributed under license from ESG.

Contents

Introduction

As a small business[1] owner, you've put your heart and soul into your business. The lifeblood of your business is data: customer data, as well as data about your intellectual property and how you run your business. Cybersecurity attacks threaten this data every single day. Small enterprises like yours struggle to allocate budget and retain resources to avoid security incidents that might compromise what you've worked so hard to create. Basic security hygiene is hard enough given resource constraints, but critical threat detection and response (TDR) is even harder.

As you probably know, small businesses are not immune to cyber-attacks. In fact, businesses like yours are a regular target for hackers, cyber-criminals, and the like. Many companies like yours seek outside assistance with cybersecurity through managed service providers (MSPs). In fact, according to a recent ESG research study, 38% of small organizations use managed security services and another 37% that do not use these services today plan to in the next 12 months.[2] These service providers include offerings that range from managing your entire IT operation to providing security functions and threat detection and response capabilities. MSPs have compelling capabilities for small business owners. They see a wide gamut of company infrastructures and crowdsourced threat data from them and provide platform-based solutions that are simple to use. These services can free you up to do what you've dedicated your life to rather than becoming a cybersecurity expert to protect your infrastructure.

This white paper outlines how MSPs rely on ESET's security offerings to satisfy small enterprise security requirements and how MSPs make it easy for small businesses like yours to stay secure.

Why Cybersecurity Matters

Cybersecurity Threats Are Real and Small Businesses Are Increasingly at Risk

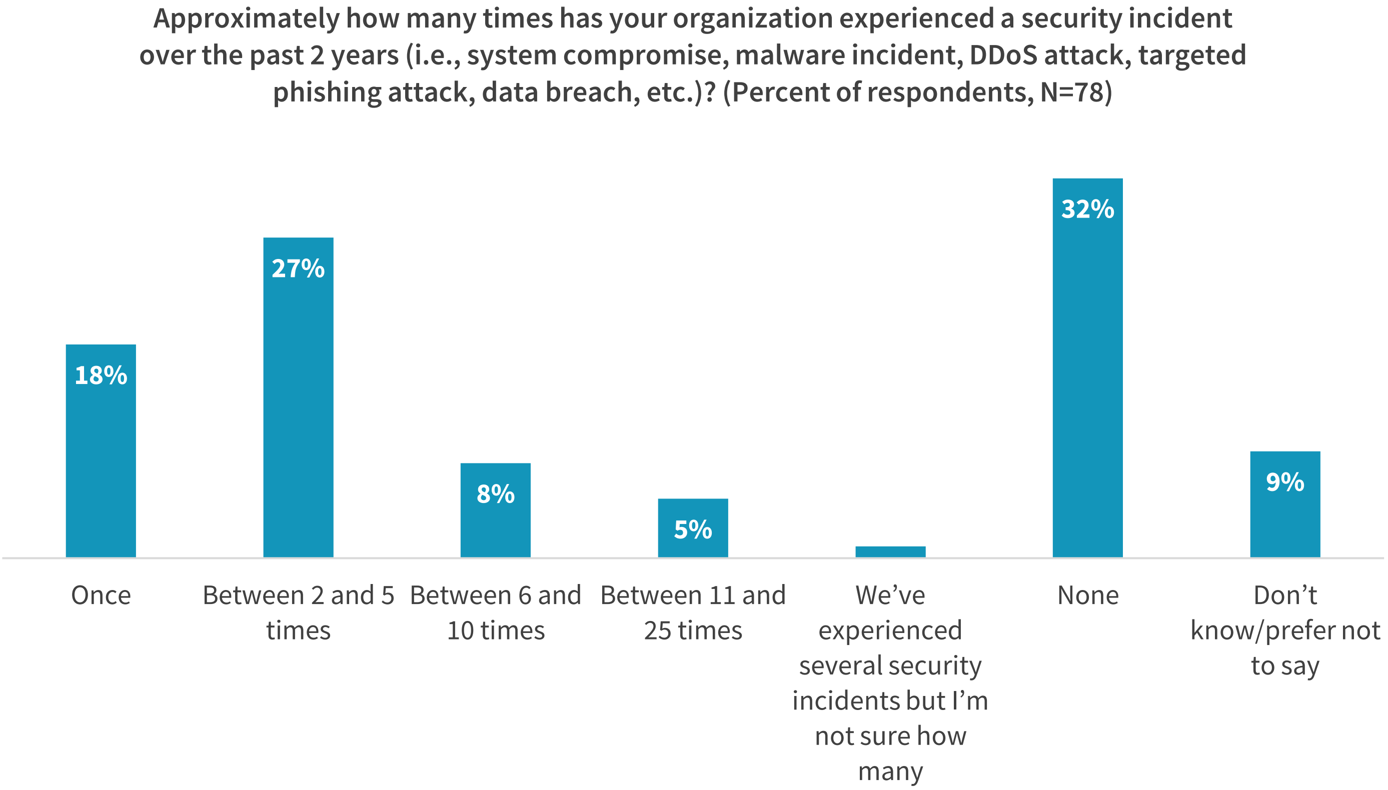
Small organizations like yours are relatively easy targets. According to Verizon's *2019 Data Breach Investigations Report* (DBIR), 43% of breaches in the past year involved small businesses.[3] When ESG asked small businesses approximately how many times their organization experienced a security incident over the past 2 years, 53% of them said they had suffered an attack between one and 10 times (see Figure 1). These incidents might include system compromises, malware, DDoS attacks, targeted phishing attacks, data breaches, and the like. Additionally, small businesses may be vulnerable to supply chain insecurity and their endpoints could become weaponized in DDoS attacks. Many of your small business brethren have seen compromised email accounts as well.

Malware and Phishing Hit Hardest

Of all attacks, small businesses feel that malware and phishing are the most disruptive.

[1] For the purpose of this paper, we use small business to refer to organizations with under 100 employees.
[2] Source: ESG Master Survey Results, *Cybersecurity Trends at SMB Organizations*, August 2018. All other ESG research references and charts in this white paper have been taken from this master survey results set, unless otherwise noted.
[3] Source: Verizon, *2019 Data Breach Investigations Report*.

Figure 1. Small Organizations Suffer Security Incidents Too



Source: Enterprise Strategy Group

Key Business Trends Impact Small Business Cybersecurity

Your business may be cloud-native, like many small businesses, meaning business systems are built on public and private cloud or multiple cloud infrastructures. However, some small companies also build their infrastructures on-premises, creating a complicated architecture in which to practice TDR. Twenty-two percent of ESG survey respondents claim new IT initiatives such as cloud and mobile computing that were implemented without proper cybersecurity oversight and controls were a factor in the cybersecurity incidents experienced. Another factor cited by 15% of the respondents was the fact that business and executive management tend to treat cybersecurity as a low priority, and 17% said that spending on cybersecurity products and services is inadequate. But interestingly, the highest contributor to security incidents, reported by a total of 46% of ESG's survey respondents, is human error (see Figure 2).

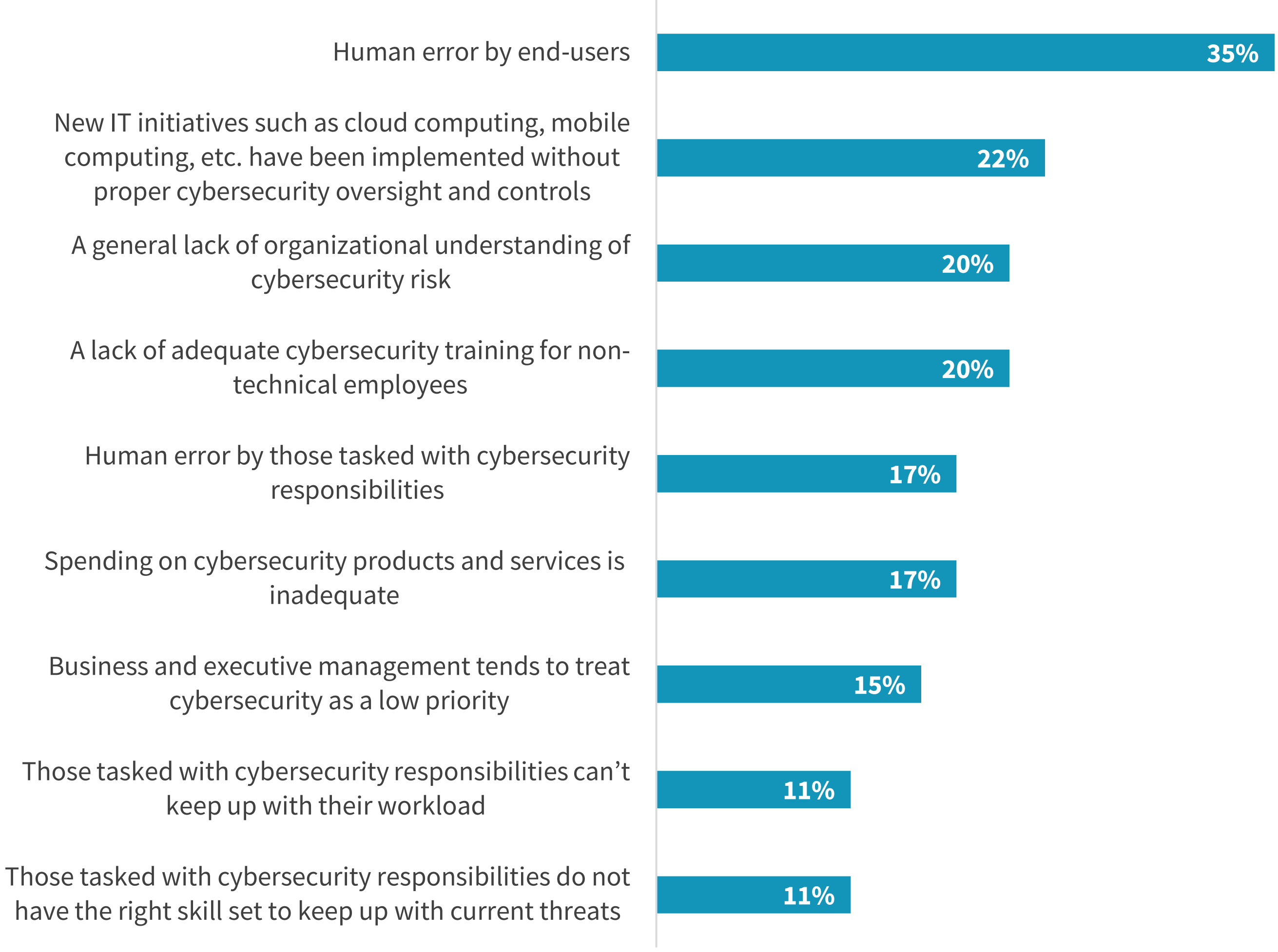
Human Error Tops Reasons for Incidents

35% cite human error by end-users.

17% cite human error by those tasked with cybersecurity responsibilities.

Figure 2. Security Events Exacerbated by Human Error, Management Priorities, and New IT Initiatives

Which of the following factors were the biggest contributors to the security events your organization experienced in the past two years? (Percent of respondents, N=46, multiple responses accepted)



Source: Enterprise Strategy Group

Human and Budgetary Resources Are in Short Supply

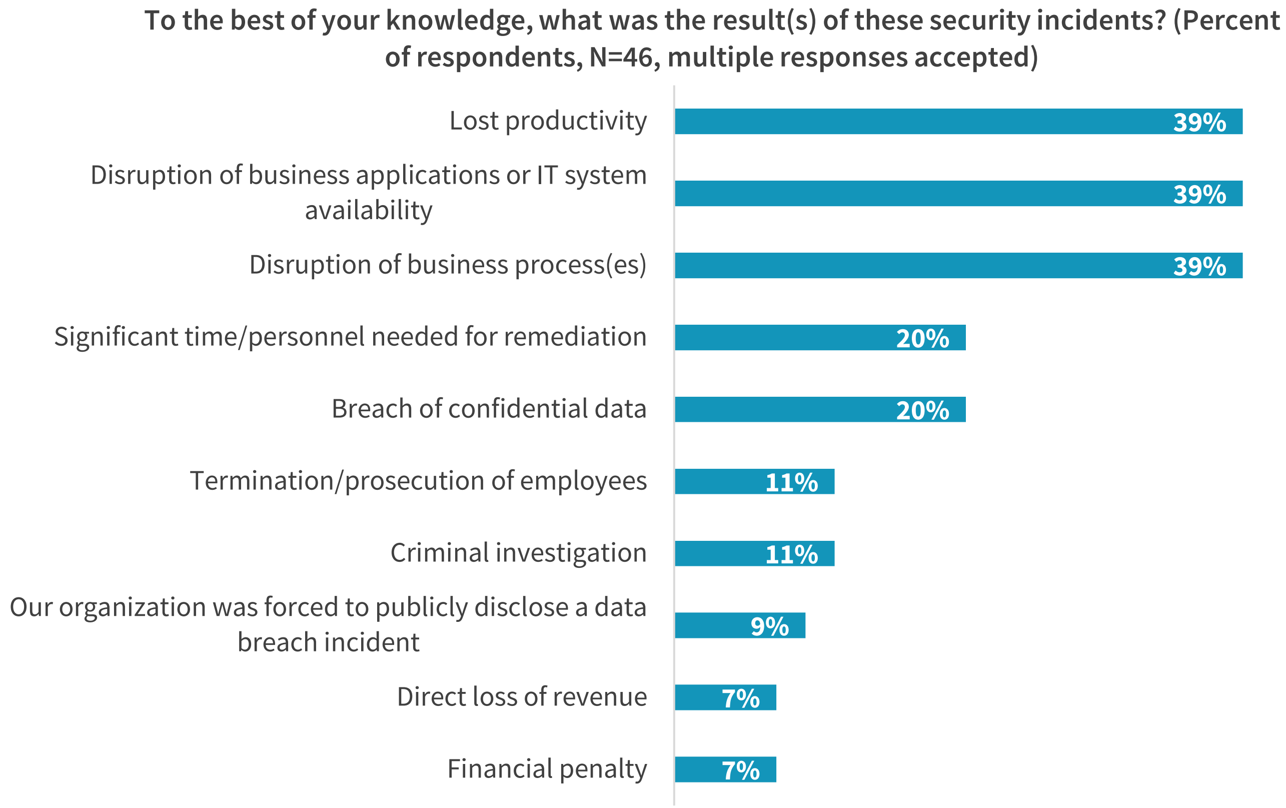
It's possible that your business struggles—like other small companies—to find enough staff to cover both the day-to-day IT operations and the rest of its overarching IT operations duties. In fact, lack of human and budgetary resources is one of the biggest challenges for the small-sized organizations. Forty-eight percent of small businesses surveyed corroborate that their IT staff wears multiple hats, including cybersecurity. Add to this the fact that 76% of respondents to a separate ESG research study indicated that TDR is more difficult than it was 2 years ago for all sized customers, and among the reasons that respondents believe that the difficulty has increased are that the volume and sophistication of threats and the TDR workload has increased.[4] This is relevant to your small enterprise especially because TDR requires specialized staff you might not be able to find or afford.

[4] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

Breaches Damage the Business

As you know, security breaches can damage your business, and companies like yours have more to lose and aren't able to recover as easily. Ineffective security creates business risks such as lost productivity; disruption of business processes, applications, and IT systems; as well as breaches of confidential data, which as we've discussed is the lifeblood of all enterprises, but the loss of which can decimate a small business (see Figure 3).

Figure 3. Lost Productivity, Disruption of Business and Systems, and Loss of Data Top Breach Outcomes



Source: Enterprise Strategy Group

Enter Managed Service Providers (MSPs)

Outsourcing cybersecurity to an MSP that offers security technologies and services specific to small businesses, like those offered by ESET, ensures that basic security hygiene is practiced, security operations are monitored, and your company gains visibility into alerts and possible intrusion, thereby reducing potential for disaster. In addition, buying security through subscription-based services removes the need for you to buy security technologies outright. Small enterprises look to outsource TDR and to purchase hands-on response and remediation, threat containment, and risk management for the organization. This is often called managed threat detection and response (MDR). Additionally, threat management and 24x7 support staff are top of mind for the small enterprise.

Due to the dearth of dedicated cybersecurity staff in small organizations, security behavior falls to all employees. According to ESG research, more than two-fifths of small company respondents believe more cybersecurity training to nontechnical employees would provide the biggest cybersecurity benefit for their organization moving forward. Many MSPs offer security employee training toward this end.

How to Evaluate and Engage with an MSP

Security technologies critical to a small enterprise include endpoint protection and encryption along with endpoint detection and response tools, or EDR. Two-factor authentication is table stakes for small businesses to ensure proper user access and authentication of systems. Beyond these two requirements, it is useful to consume these services via a platform that is reliable and simple to deploy. Ease of use removes obstacles to small businesses that might not have the time and resources to fully understand and manage security capabilities.

Questions to Consider when Evaluating an MSP

- Does the MSP have a broad range of products and services available to small businesses specifically?
- What assistance is provided to assess the organization’s infrastructure, and implement any and all technologies? What can the MSP offload operationally for the company?
- Finally, how available are the MSP maintenance and support staff to the client?

Ultimately small businesses are just like any other businesses regarding cybersecurity hygiene, employee training, and top-notch service. However, small businesses do need more handholding because their employees are forced to wear so many different hats. They also need a service provider that understands the cybersecurity issues that small businesses face and can assist them in making the right technology decisions. Small businesses need to keep costs down without sacrificing quality and ease of use, which can free them up to concentrate on running the business.

The Bigger Truth

Reducing cybersecurity risk should be a high priority, but it’s not easy, especially for small-sized firms. Cybersecurity is made more approachable, manageable, and effective with the right support and full range of MSP services predicated on solid security technologies from a reliable vendor, such as ESET, that focuses on MSP excellence. Both ESET and its MSP partners understand small businesses like yours and where your company needs the most cybersecurity help: endpoint protection and encryption, two-factor authentication, EDR, and MDR. TDR is challenging for firms like yours because small enterprises are short-staffed and under-resourced. Hence, turning to MSPs engaged in a strong vendor partnership with a company like ESET can assist you to get back to business and leave cybersecurity to the experts.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.