SilverSky

How to Avoid $22 Million in Cyberattack Costs

SMB's guide to cost-effectively securing your organization

How to Avoid $22 Million in Cyberattack Costs

SMB's guide to cost-effectively securing your organization

The increasingly digital economy has fostered incredible opportunities, along with many new areas of risk. Given the tremendous levels of digital transformation, cybercrime has quickly become today's fastest-growing form of criminal activity. Small- and medium-sized businesses (SMB) are especially at risk with 43 percent of online attacks now aimed directly at them because cybercriminals know that SMBs are often softer targets.[1]

The average costs of cyberattacks vary by industry but averaged $13.0 million in 2018.[2] The banking industry is particularly exposed with cybercrime costing $18.4 million per company and increasing approximately 11 percent per year.[3] In 2020, organizations in exposed industries will each incur more than $22 million in cyberattack costs if strong defensive plans are not in place.

The opportunities for cybercriminals reside in the fact that today's IT infrastructures are more complex and sophisticated than ever, and there are a multitude of devices and communication pathways exponentially increasing the attack surface to be managed.

Sophisticated ransomware, smartphones being used for surveillance attacks, refined decoy environments, hardware and firmware attacks, DNS spoofing, phishing attacks, IoT breaches, cloud security incidents, distributed denial of service (DDoS) attacks – the list goes on and on. Not only is the list of cybersecurity vulnerabilities long, but an immense assortment of technical skills is also required to address them. The lack of technical skill and technology resources is why SMBs are so exposed. Cybercriminals know that SMBs cannot afford the full range of technologies needed to protect their organizations.

Alert triage can simply overwhelm small security teams, and research shows many teams only respond to approximately half the alerts they see on a daily basis. And with 41 percent of organizations seeing more than 10,000 alerts every day[4], too often, the doors are wide open for attackers.

The inevitable cyberattack will not only lead to lost productivity and revenue but also a potential liability, regulatory noncompliance, and reputational damage. To gain further insights, SilverSky surveyed our customers – primarily SMBs in the financial services, healthcare, and retail industries –to learn more about their concerns. A range of concerns was reflected in the results with network and device vulnerabilities and email vulnerabilities at the forefront.

> "In 2020, organizations in exposed industries will each incur more than $22 million in cyberattack costs if strong defensive plans are not in place."

4 Cybersecurity Challenges Pressuring Small- and Medium-Sized Companies

As mentioned, SMB's are favorite targets for cybercriminals due to higher rates of vulnerability. What are some of the specific factors creating these areas of exposure?

Velocity, Creativity, and Sophistication of Attacks

Ever-expanding technological sophistication provides a growing opportunity for organizations to expand their service offerings, better serve customers, reduce operational costs, and deliver many other value points. However, cybercriminals have also become much more sophisticated. Attackers will utilize a wide variety of tools, strategies, and technologies to attack the expanding technology infrastructure of their targets. Due to this growing frequency and sophistication of attacks, organizations' ability to anticipate and prevent attacks has been dramatically reduced.

Cost and Availability of Cybersecurity Talent

Because IT systems have become so much more sophisticated and specialized, the cybersecurity expertise needed to protect an organization is diverse, expensive, and in short supply. The need for greater numbers of cybersecurity professionals has been reported in numerous industry reports. Specifically, a recent Cybersecurity Ventures report predicted that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, approximately 500,000 of those unfilled positions will be in the United States.[5] This talent shortage and the rising costs of securing cybersecurity talent is a large challenge for SMBs.

Rapidly Expanding Perimeter

Organizations need to think about their perimeters much differently today. Countless additional endpoints, including mobile devices and IoT-enabled devices have greatly expanded the area we need to protect.

Regulatory Requirements

Regulatory data protection and privacy challenges will continue to grow primarily in response to the constant demand for more personal data to deliver newly created products and services.

> Cybersecurity Ventures report predicted that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, approximately 500,000 of those unfilled positions will be in the United States.[5]

MDR, MSSP, EDR – What's the Difference?

Once you have decided to find a cybersecurity services partner, which direction should you go? There are three approaches to consider – Managed Security Services, Endpoint Detection and Response, and Managed Detection and Response solutions. But, among these directions, what are the differences, and which is the best solution for your organization's cybersecurity?

Managed Security Services

Managed Security Service Providers (MSSPs) usually function to off-load monitoring and management tasks from internal security teams and send alerts when threats are identified. MSSPs provide a traditional passive network defense approach. While this approach is a necessary component of any security plan, the evolution of cyber threats necessitates changes in the way companies approach cybersecurity. The breadth and depth of new threats require a broader set of skills and a deeper level of engagement than many MSSPs can provide.

Endpoint Detection and Response

An increasingly mobile workforce has added millions of new devices to corporate networks. These mobile devices need to be secured, just like devices inside the network, to avoid creating new security vulnerabilities. The reality is, the incredible number of endpoints defines the new perimeter. In response to this new state, a new set of vendors providing Endpoint Detection and Response (EDR) solutions have emerged. Robust EDR has become an essential component of effective cybersecurity, but EDR must be paired with dynamic UTM perimeter and extended network monitoring to secure an organization properly.

Managed Detection and Response

One key to a successful cybersecurity plan is to have layered defenses that address multiple threats, and this is where an Managed Detection and Response (MDR) provider shines. MDR services allow you to not only monitor more of your attack vectors, they also help you take steps to stop the attack, remediate the assets that have been attacked and protect them from being attacked again.

The skills shortage in cybersecurity combined with the high costs of technology makes it challenging for any company to deploy and manage their internal MDR function. Even if they were able to do it, they would still lose the combined intelligence that comes from protecting thousands of companies that are exposed to a vast number of threats. By using superior technology and expertise gathered in the trenches every day, MDR providers can provide superior service at affordable prices.

Reduce Cyberattack Costs with Managed Detection and Response (MDR)

You're going to be attacked. This is not the reality anyone wants to acknowledge, but it's true. Unfortunately, many organizations are still setting goals and assigning resources intensely focused on preventing cyberattacks.

Yes, do everything you can to avoid exposing your company to attacks. But effective approaches today must center on monitoring the organization's expanded attack surface area, detecting attacks as quickly as possible, and swift remediation.

Remember, each organization in more exposed industries, like financial services, will incur more than $22 million in cyberattack damage per year without adequate monitoring, detection, and remediation strategies in place.

Managed detection and response (MDR) is an increasingly popular approach that addresses these security monitoring and remediation challenges, as it delivers real-time, 24x7 managed detection and response using a holistic, turnkey approach. As a cost-effective alternative to building an in-house security operations center (SOC), MDR protects against advanced threats both within and outside of traditionally defined perimeters, facilitates remediation when security breaches do occur, and enables organizations of all sizes to follow cybersecurity best practices even given resource constraints.

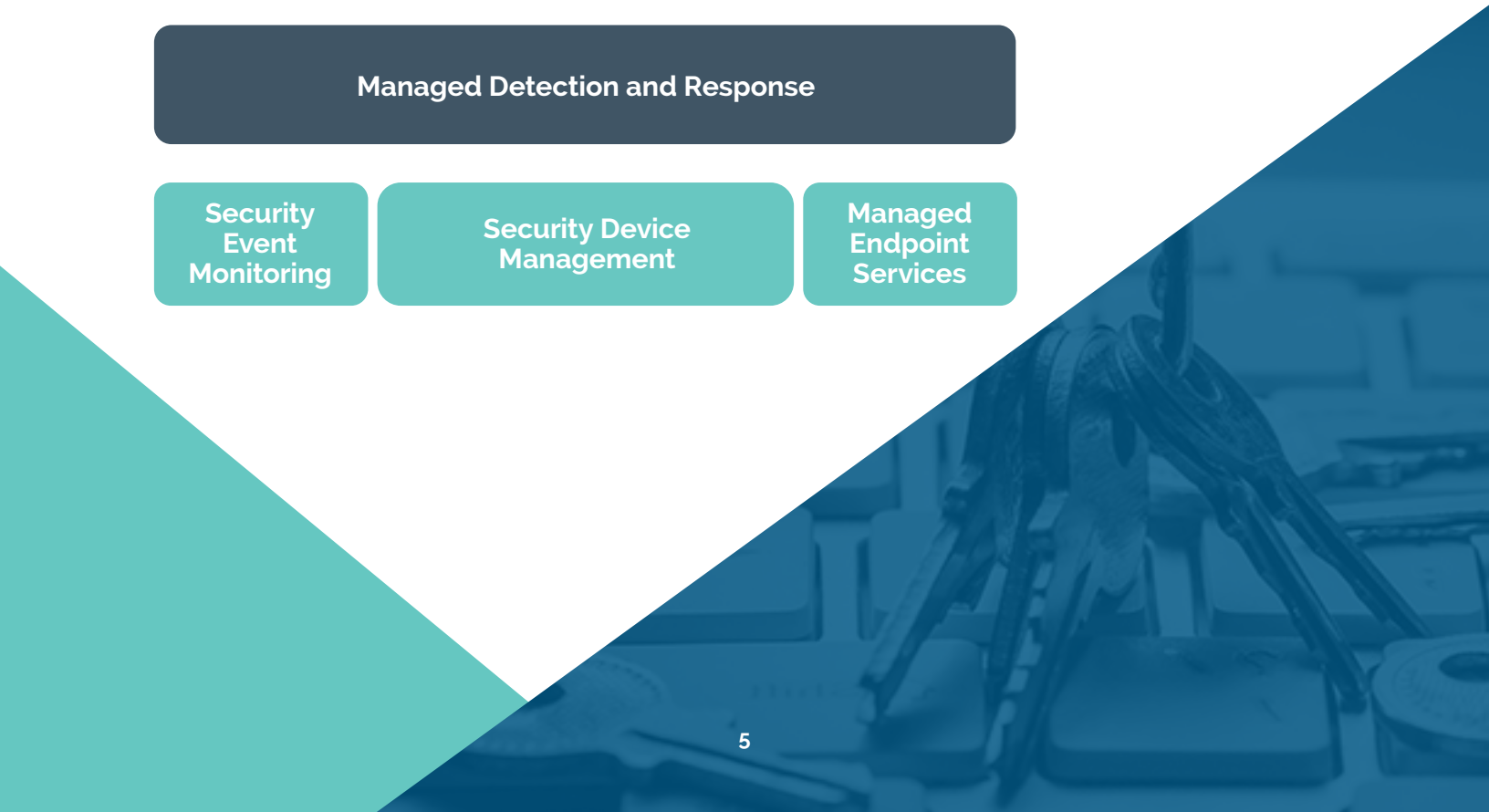
SilverSky's Managed Detection and Response offering provides around the clock monitoring and management of your cybersecurity infrastructure. Our trusted, cybersecurity experts have the education and practical experience to help your security team separate significant threats from false positives and make sure your infrastructure is up-to-date and optimized to perform at its best. We will monitor your unified threat management devices, intrusion detection and protection service, web content filtering, web application filtering, gateway anti-virus as well as your domain name servers, and active directory servers.

Managed Detection and Response

Security Event Monitoring

Security Device Management

Managed Endpoint Services



Selecting the Right MDR Partner for Your Organization

Once you have decided that choosing an MDR partner is the right direction for your company, how do you select the partner that is right for you? The following are some questions you should ask.

What is their heritage?

Have they been in the cybersecurity business at the highest levels for a long time? Have they been able to secure and maintain the talent and technology to protect you from the most sophisticated threats? Many vendors, notably smaller regional providers, have evolved from other business models. Managed detection and response takes time to develop the tools and expertise to be effective. You don't want to be a training ground for new entrants.

What markets do they serve?

Regulated industries are regulated for a reason. They have high-value assets that need to be protected more stringently than most commercial companies. If your MDR provider supports financial services, healthcare, retail, and other industries that have substantial compliance requirements, you can rest assured that they have technologies, skills, and expertise to get the job done.

When are they available?

To remain safe, you need an MDR partner that is watching over your company 24x7x365 with a solid plan for discovering, triaging, alerting, and responding to threats. Because threats can come from anywhere in the world at any time, you need to have active, real-time surveillance of all of your attack vectors.

Do they know the latest threats?

The right MDR partner will have the threat intelligence available to be proactive against the latest threats before they become a problem for your business.

Do they have the right technology and the right people?

Your MDR partner has to be continually investing in the latest technologies to stay a step ahead of cybercriminals. But, technology alone won't make you safe. Couple that technology with trusted cybersecurity experts that understand your business and are easy to work with to get to the highest levels of security.

Will they help plan your defense?

Even with the best security, attacks can happen. Your MDR partner should have services available to help plan your incident response so that everyone involved knows what to do to minimize the impact of an attack and to restore everything to normal as quickly as possible.

MDR Glossary of Terms

MDR is a new term coined by analysts with quick adoption by cybersecurity vendors as the next step in securing your company and your data. MDR has brought with it other terms that may be new to you, so we've compiled an MDR glossary to help.

Antivirus (AV)/Anti-Spam: Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more. With anti-spam software, emails that have suspicious content are flagged and then immediately sent into a spam folder, instead of going into the regular inbox.

Endpoint Detection and Response (EDR): A second-generation endpoint security solution focused on advanced threats, including continuous monitoring and response. Endpoint detection is sometimes sold as a stand-alone product but is more effective when combined with an MDR solution for a layered defense.

Firewall: A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and an untrusted external network, such as the Internet.

Intrusion Detection System (IDS): A hardware or software appliance that provides real-time monitoring of network traffic and creates automatic alerts upon detection of indicators of compromise (IOCs).

Incident Response (IR): An organized, systematic approach to addressing the impacts of a security incident or data breach to limit the damage to the infrastructure and the business.

Managed Detection and Response (MDR): A comprehensive service for continuous monitoring, infrastructure management, threat detection, and incident response provided by a third-party vendor.

Managed Service Provider (MSP): An IT vendor that provides a service, software, or technology, such as remotely managing IT infrastructure, on a subscription basis.

Managed Security Service Provider (MSSP): A company that provides 24x7 management, monitoring, and maintenance of security services, such as firewalls, intrusion detection, and prevention systems, and other security solutions at a fixed subscription cost.

Security Information and Event Management (SIEM): An integrated system that combines security information management and security event management to collect and correlate security events and alerts.

SOC (Security Operations Center): A centralized approach that combines security technology, people, and processes to manage threats—from prevention and detection to investigation and response.

Threat Hunting: Proactive searches of data to identify stealthy threats that have evaded perimeter controls and are hiding on the network or endpoints.

Threat Intelligence: Evidence-based data about current and potential threats, including context, indicators of compromise, mechanisms, and actionable information.

Unified Threat Management (UTM): A category of security appliances that integrates a range of security features into a single appliance. UTM appliances combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single platform.

Web Application Firewall (WAF): A WAF filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF can filter the content of specific web applications while regular firewalls serve as a safety gate between servers. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

Web Content Filtering: Web content filtering can prevent people in your organization from accessing web pages that may harbor computer viruses or malware, or from viewing inappropriate material that could lead to HR issues. By preventing access to selected web pages, web content filtering solutions can strengthen an organization's cybersecurity defenses, increase productivity, and avoid HR issues before they begin.

SilverSky's Managed Detection and Response Solution

From the data center to the endpoint, SilverSky's Managed Detection and Response solution provides end-to-end protection

Core security devices like Unified Threat Management, Active Directory, Domain Name Servers, Endpoints and more are configured to send security events to the proprietary SilverSky Threat Detection platform

Devices are monitored for uptime, health, and effectiveness, configured for optimal security and updated based on real security threats to the organization

Our cybersecurity experts monitor and manage your devices giving you early visibility into threats and performing actions to mitigate them

Data is correlated and compared across all devices and feeds by extensive detection capabilities and threat intelligence

Analysts provide active response and remediation to assist your team in resolving issues as appropriate

SilverSky's MDR solution is built on twenty years of experience working with small- to mid-sized businesses in both regulated and unregulated industries. We have the technology, resources, and expertise to give you peace-of-mind and a healthy return on your cybersecurity investments. Contact us to learn more.

Sources:

1. "Cyberattacks now cost companies $200,000 on average, putting many out of business," Scott Steinberg, CNBC.com, October 13, 2019
2. "The Cost of Cybercrime, The Ninth Annual Cost of Cybercrime Study," Accenture, March 2019
3. "This is the crippling cost of cybercrime on corporations," Iman Ghosh, World Economic Forum, November 7, 2019
4. "2019 CISO Benchmark Study," Cisco
5. "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021, Steve Morgan, Cybercrime Magazine, October 24, 2019

SilverSky

www.silversky.com

Contact Details: US: 1-800-234-2175 | E: learn@silversky.com
SilverSky, 4813 Emperor Boulevard, Suite 200
Durham, North Carolina 27703
linkedin.com/company/silversky | twitter.com/SilverSky