E-BOOK / CISCO POWERED SECURITY

A View of the Cybercrime Threat Landscape

and How SMBs can Help Protect Themselves with Cisco Umbrella with Cisco Powered Security

networkiq

cisco Security

$2,235,018 per year

The average amount SMBs spent in the aftermath of a cyber attack or data breach due to damage or theft of IT assets and disruption to normal operations*

The amount is staggering, and enough to jeopardize the viability of many companies. Yet the business benefits that come with the internet, Cloud computing and other applications are impossible to forego and remain competitive. That's why business owners and executives are asking one question:

Is our internet safe?

If your service provider can't demonstrate how it is making your company less likely to become a victim of cybercrime, then it is time to consider alternatives.

Cisco Umbrella can help protect your business from online and cyber threats

On the following pages, we'll outline what companies are up against today, and how Cisco Umbrella can help bring you peace of mind.

Ransomware is on the rise

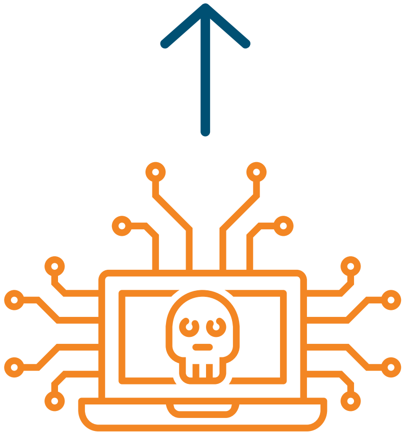
Fifty-two percent of the SMBs—participating in the Ponemon Institute's *2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) report*—experienced either a successful or unsuccessful ransomware attack in a 12 month period. And of those SMBs that were attacked, 53 percent were targets of ransomware more than twice. Yet just two percent of participants in the previous report were victims of ransomware.*

The explosion of ransomware incidents in 2016 may be due to the evolution of the ransomware business model. Cybercriminals, who developed ransomware for their own use, now run it as an affiliate program, providing low-cost Ransomware-as-a-Service (RaaS) to others in return for a share of the ransom payments.[1]

Socially engineered malware and data-encrypting ransomware are the top cyber attack methods businesses are likely to face, according to security advisor and columnist, Roger A. Grimes.[2] Ransomware, a type of malware, takes advantage of human and technical flaws in order to deny businesses, organizations, or users access to their data and systems.

Delivered through phishing, spear phishing, Remote Desktop Protocol or other vectors, ransomware can result in the rapid encryption of valuable files on a corporate network or loss of access to the network. The cybercriminal responsible for the attack demands a ransom—usually in a virtual currency such as Bitcoin—in exchange for restoring access to the encrypted data and network. The extra kicker: cybercriminals don't always honor their agreements, and demand additional payments from their victims.

(cont.)



750%

increase in ransomeware incidents over the previous year[2]

Cybercrime is organized crime

The Crime-as-a-Service (CaaS) business model was a topic at the 2017 Internet Organized Crime Threat Assessment, presented at the annual Europol-INTERPOL Cybercrime Conference at The Hague in September of 2017.[3]

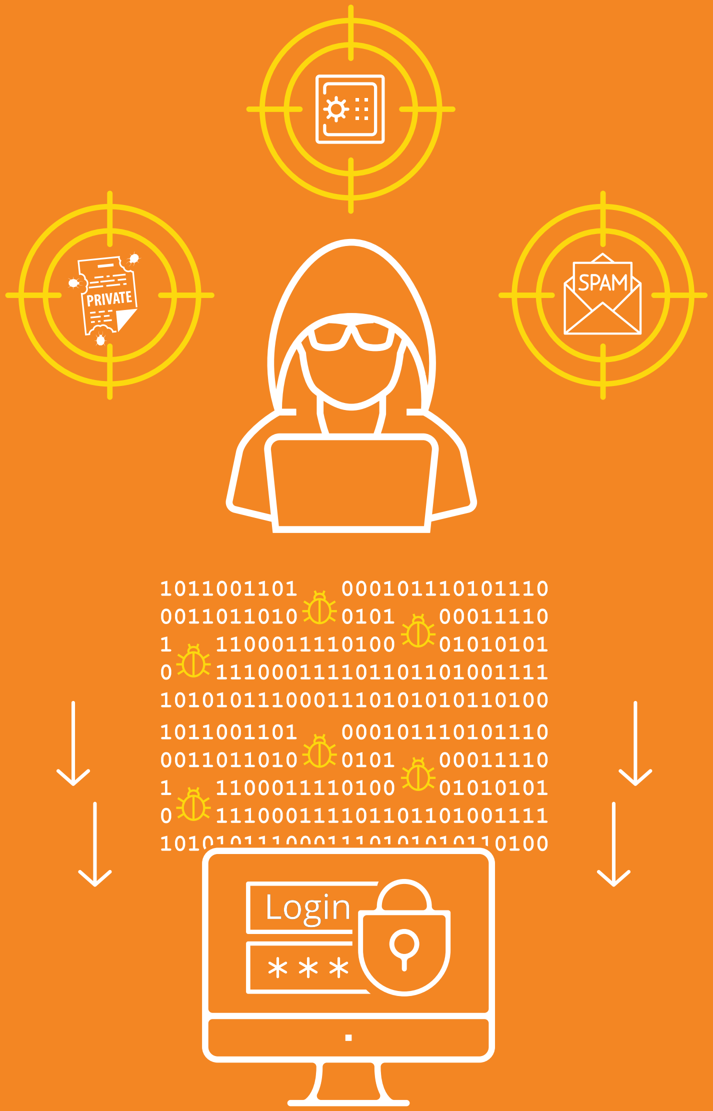
CaaS and RaaS enable cybercriminals to specialize in specific skill-sets, while gaining access on an as-needed basis to cybercriminals with different skills to conduct identity theft, ransomware and other forms of cybercrime. This method allows cybercriminals to operate successfully with minimal expertise and investment, as well as empowers them to commit crime as a coordinated group.

New developments in ransomware make it more troublesome for companies of all sizes

Instead of requiring a recipient to open an emailed attachment or click on a link, current trends in ransomware—such as *WannaCry*, which began in May 2017—appear to enable them to easily transmit themselves without user interaction and between networks. "*WannaCry* is the first one to completely automate," says Craig Williams, a senior security outreach manager at Talos, the security research arm of Cisco.[4]

WannaCry affected more than 200,000 computers worldwide, including those belonging to FedEx, and may cause an estimated $4 billion in losses.[5] However, the initial *WannaCry* attack could've been more severe in the U.S. and elsewhere. Marcus Hutchings, a security researcher in the U.K., accidentally discovered a 'killswitch' that slowed down the spread of *WannaCry*.

(cont.)



Nevertheless, new forms of cyberattacks are coming

SMBs can be vulnerable to attacks from *NotPetya*, another type of ransomware that targets Microsoft Windows PCs. Merck, an American pharmaceutical company with a large enterprise-grade IT department, could not cope with the attack and was held for ransom by *NotPetya*. More recently, a new strain of *WannaCry* attacked FirstHealth of the Carolinas, a North Carolina-based health system. And at the time of writing this paper, a new ransomware variant called *Bad Rabbit* appears to be attacking organizations in Russia, Ukraine, Turkey, Germany, Bulgaria, and Japan, and has been detected in the U.S., South Korea and Poland.

Increased insurance costs

Insurers could pay Merck up to $275 million to cover the insured portion of its losses from its *NotPetya* cyber attack, prompting companies of all sizes to consider devoting resources to pay for cyber crime insurance. Tryg, an insurance company headquartered in Denmark, expects 90 percent of its corporate customers to buy cyber crime insurance within five years due to the growing threat from hackers and viruses. After launching its new data recovery and business continuity (DR/BC) services at the beginning of 2017, Tryg has sold 5,000 cyber crime insurance policies. Tryg CEO Morten Hubbe says just as all corporations today have insurance on their buildings or cars, that within a very few years they will also insure against cyber crime.[6]

▸ THE COST OF RANSOMWARE IS MORE THAN THE RANSOM

Companies that pay ransom fees soon realize that the associated costs can outweigh the ransom. After making a $25,000 ransom payment, the Lansing Board of Water & Light acknowledged the full extent of its costs: responding to and recovering from the attack reached $2.4 million.[7]

The reason behind the additional expense is that despite the ransom amount appearing relatively low, a ransomware attack requires an immediate response by a cyber emergency team. Even if they can restore the system without paying the ransom, and prevent future attacks, the total cost can escalate beyond the initial demand.

In the Lansing Board of Water & Light's case, the ransomware shut down the utility's email and accounting systems as well as affected phones, computers, printers and other technology after an employee opened an email with an infected attachment. It took approximately a week for the utility to recover.

HOW WELL COULD YOUR COMPANY HANDLE A CYBERCRIME ATTACK? **SEE NEXT PAGE.**

Companies that fail to protect customer data make the news

A single security breach can destroy the trust your company worked hard to gain. A breach may also result in negative press, lawsuits, loss of propriety information, and a loss of customers. And as your company increasingly relies on the internet for a wide range of business activities, it must ensure that it is doing all it can to maintain online security.

How would a security breach or a ransomware attack affect your business?

- What is the potential financial impact of a network outage due to a security breach, or loss of access to data and systems due to a ransomware attack?
- Could a security breach or ransomware attack disrupt your supply chain?
- What would happen if an attack caused your website to go down?
- Does your company rely on e-commerce features on its website? How long could the site be down before your business lost money?
- Is your company insured against cyber attacks, or against the misuse of your customers' data? Is this insurance adequate?
- Does your company have backup and recovery capabilities to restore information, if necessary, after a security breach or loss of data due to a ransomware attack?

▸ WHAT ARE YOUR EMPLOYEES UP TO?

Of the respondents participating in the Ponemon Institute's 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) report that experienced a data breach, 54 percent say negligent employees were the root cause—an increase from 48 percent of respondents in last year's study.*

Robust passwords continue to play an essential role in SMB cybersecurity. Yet 59 percent of respondents in the current Ponemon report—the same percentage as the previous report—say they do not have visibility into employee password practices, including the use of unique or strong passwords.*

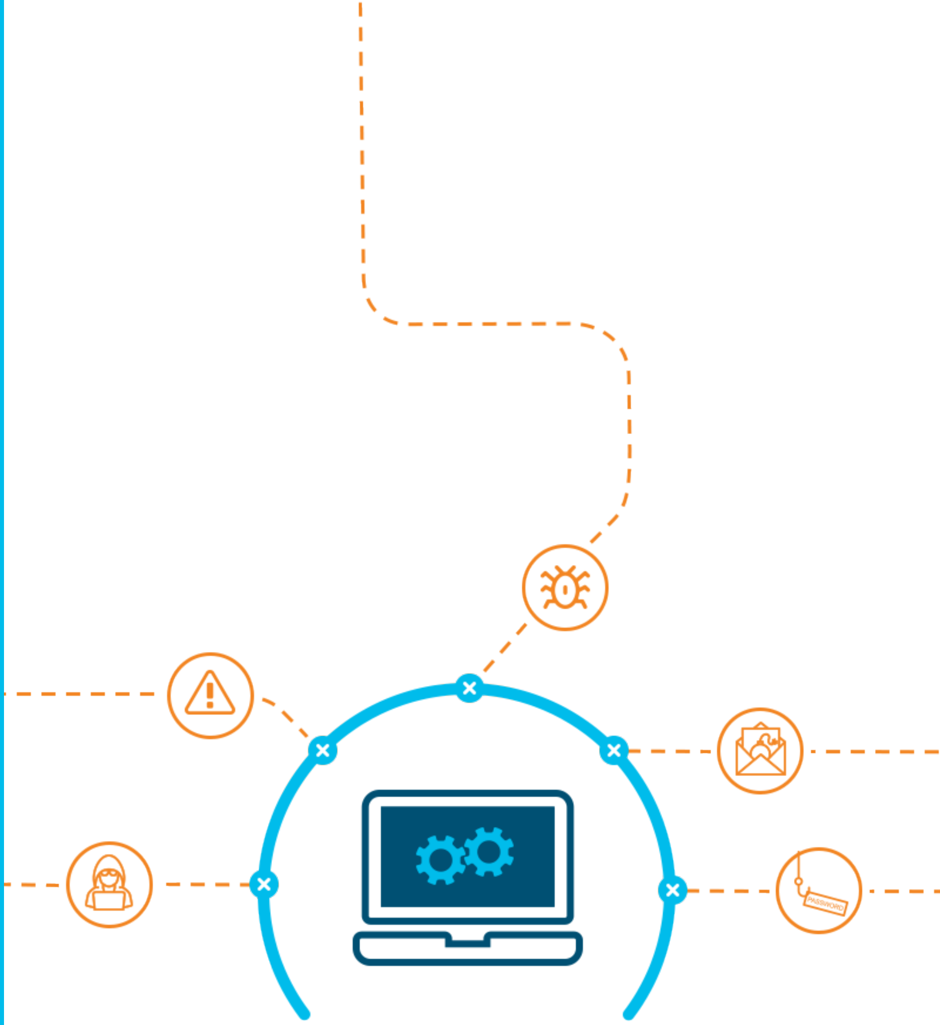
Respondents also say that password policies are not strictly enforced. If a company has a password policy (43 percent of respondents do), 68 percent say it is either not strictly enforced or they are unsure how well it is administered.*

NEED A SOLUTION TO HELP SAFEGUARD YOUR COMPANY FROM CYBERCRIME? **SEE NEXT PAGE.**

A cloud security service that provides built-in protection for your internet service

Cisco Umbrella is a cloud security service that provides built-in protection against attacks over your internet connection, helping you mitigate the time and cost spent dealing with cyber attacks. The solution provides proactive protection against threats on the internet, such as malware, botnets and phishing attacks. It helps keep your business safe by delivering clean traffic before it reaches your internal network, effectively learning where attacks are being staged, and blocking threats over all ports and protocols. You can be confident that with secure internet access, you are protected with a first layer of defense against malware.

WANT TO KNOW MORE? SEE NEXT PAGE.



Cisco Security

SOURCE: * Ponemon Institute. "2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)." http://www.veille.ma/IMG/pdf/2017_state_of_cybersecurity_in_small_medium-sized_businesses.pdf (Accessed November 2, 2017)

[1] Conner, Bill. "Ransomware-As-A-Service: The Next Great Cyber Threat?" Forbes.com. https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#4063df8c4123 (accessed October 25, 2017)

[2] Grimes, Roger, A. "The 5 cyber attacks you're most likely to face." Csoonline.com https://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html#tk.csoendnote (accessed October 24, 2017)

[3] Europol. "The 2017 Internet Organized Crime Threat Assessment (IOCTA)." Europol.europa.eu. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (accessed October 24, 2017)

[4] Weise, Elizabeth and Snider, Mike. Usatoday.com. https://www.usatoday.com/story/tech/news/2017/05/15/ransomeware-attack-wannacry-malware/101710900/ (accessed October 24, 2017)

[5] Berr, Jonathan. ""WannaCry" ransomware attack losses could reach $4 billion." Cbsmew.com. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (accessed October 25, 2017)

[6] Kass, DH. "Mercks Notpetya $275 Million Loss Could Prompt Rise in Cyber Insurance." Msspalert.com. https://www.msspalert.com/cybersecurity-news/mercks-notpetya-275-million-loss-could-prompt-rise-in-cyber-insurance/(accessed October 25, 2017)

[7] Conner, Bill. "Ransomware-As-A-Service: The Next Great Cyber Threat?" Forbes.com. https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/2/#1ba6e5695a0a (accessed October 25, 2017)

networkiq

CISCO Security