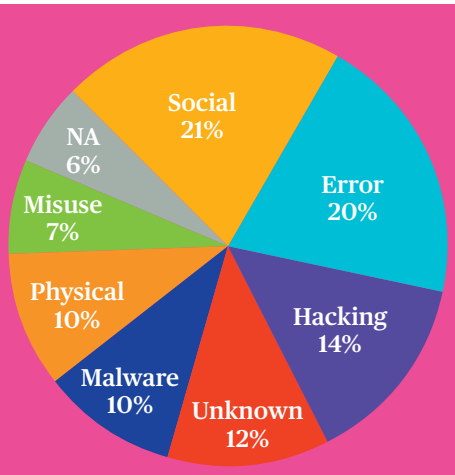
Cyber Criminals Increasingly Target Small and Midsize Businesses

Although large-scale cyber incidents garner major media focus, data shows that cyber criminals are increasingly turning their attention to smaller companies. In fact, 62% of all cyber breach victims are small and midsize enterprises (SMEs), according to Small Biz Trends.[1] Evidence shows that this trend of targeting SMEs will continue to rise. Why are smaller businesses the favored targets of cyber criminals? Most likely because bad actors know that SME leaders often mistakenly think that cyber security services are beyond their means, making them under-protected and easily breached. By monitoring trends and raising awareness of new threats, we can help our insureds reduce their exposure to close up cyber attacks, regardless of the size of their business.

Visit the Chubb Cyber Index℠ to learn about data-driven cyber trends.

"Cyber criminals typically don't target specific small businesses, but they increasingly use tools that target the *vulnerabilities* of small businesses. Those vulnerabilities are sometimes technical, like unpatched software or poorly configured hardware. Even more commonly, those vulnerabilities are simply employees who may use weak or compromised passwords, or may inadvertently click something they shouldn't have."

Patrick Thielen
SVP, Chubb
Underwriting, Financial Lines



Chubb Claims Small Business Action Statistics for 2018

Emotet – A virus leading to increased business interruption claims

What it is

Emotet is a type of malware called a banking Trojan, which is designed to steal financial information and online banking credentials.

How it works

It is disseminated through phishing emails that contain a malicious link or attachment that drops the Emotet malware on the victim's system when opened.

Trend

Chubb has seen an increase in Emotet infections in recent months. It has become more problematic for its victims because it is sometimes observed as a precursor to particularly troublesome types of ransomware (such as Ryuk, as discussed below).

Chubb Insight

While we are not seeing access to or exfiltration of personal information in these matters, Emotet infections are leading to an increase in business interruption claims because insureds are having to shut down their systems to prevent the spread of the virus. A good endpoint protection product can help detect and eradicate Emotet malware.

Ransomware Attacks – Past & Present Trends
What You Need to Know

Ransomware attacks utilize malicious software to block access to an organization's network until a ransom is paid. While we continue to see an increase in the number of ransomware attacks perpetrated, the amount of ransom demanded, and the number of ransoms paid, the most commonly used variants of ransomware are changing. Right now the latest strain of ransomware that is quickly wreaking havoc on organizations across the country is called Ryuk, which we outline below in order to keep you ahead of this trend. However, we are seeing a precipitous decline in the number of SamSam ransomware attacks, which we outlined almost a year ago in our **1Q'2018 Chubb Cyber Infocus Report**.

SamSam

We have not had any claims involving SamSam since November of 2018, when two Iranian nationals were indicted by the U.S. Justice Department for creating SamSam and deploying it on a number of victims, including the City of Atlanta and other high and low profile organizations. Unlike other types of ransomware attacks such as phishing emails, SamSam ransomware targets its victims and then exploits their networks' vulnerabilities, such as weak passwords. SamSam utilizes brute force attacks that enable bad actors to repeatedly guess a password until they gain access to the victim's computer system.

Ryuk

What it is

Ryuk is a new strain of ransomware that is particularly virulent, hard to detect, and characterized by very high ransom demands (generally above $100,000).

How it works

Bad actors typically use Emotet or Trickbot malware to infect the victim's system before Ryuk is deployed. Ryuk usually infects the victim's main systems and may hide itself as a legitimate VPN user. The bad actors encrypt the victim's data and eventually make a very large ransom demand

Trend

Ryuk is often accompanied by some type of banking Trojan software that enables the bad actor to steal the victim's financial information. We frequently see the bad actors negotiating with the victim knowing that the victim has adequate resources to pay their demands.

Chubb Insight

Endpoint monitoring can assist with detection of Ryuk ransomware. Detailed VPN logs also enable system administrators to spot suspicious activity. Employees should also be trained on how to detect suspicious email to avoid this malware. Chubb cyber panel forensic firms have been remediating this type of ransomware for several months.

Credential Stuffing – An attack that is on the rise

What it is

A type of cyberattack used to gain unauthorized access to online user accounts.

How it works

After purchasing email addresses and passwords on the dark web, an attacker uses botnets to programmatically target multiple online user accounts using the email addresses and passwords. An account becomes susceptible when a person uses the same email and password combination across multiple sites. Once the attacker gains access, they take over the account and use it to make fraudulent purchases and obtain additional personal information.

Trend

Attacks like these are on the rise and do not seem to discriminate based on size. Retailers and financial service sites are prime targets.

Chubb Insight

Credential stuffing is a threat to businesses as well as consumers. A business can incur costs to notify users whose accounts have been compromised by credential stuffing and can also be liable for any fraud arising from the attack. Whenever possible, a business with online account access should enable multi-factor authentication.

Chubb. Insured.℠

[1] SOURCE: Alton, Larry. "How to Protect Your Small Business as Cybersecurity Threats Rise." Small Business Trends: https://smallbiztrends.com/2016/06/cyber-security-strategies.html (June 3, 2016).