CHUBB®

Cyber InFocus

Fourth Quarter, 2020

No matter how large or small, every business is at risk for cyber crime.

At Chubb, we want to help you stay protected. That's why we bring you this quarterly Cyber InFocus report to help you understand how cyber and privacy-related incidents can affect your business and to assist you in preventing issues from happening in the first place.

Based on our own proprietary data, Cyber InFocus:

- Showcases the cyber crime trends we're seeing
- Provides advice on how to mitigate cyber risk
- Illustrates cyber crime stories involving businesses in the most vulnerable industries, how the cyber incidents were exposed, and what the businesses learned in the process

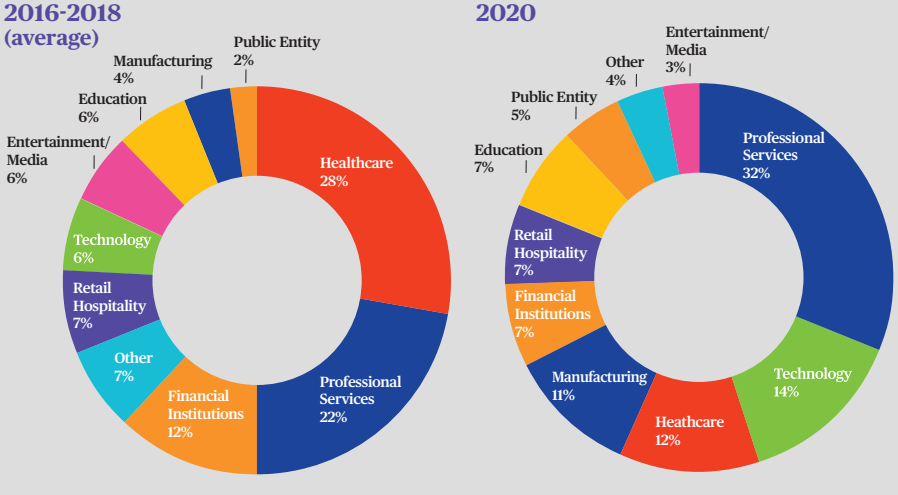
We're here to help businesses understand the cyber security industry landscape and provide them with the tools and resources they need to stay ahead.

Trends we are seeing:

Cyber Risks in Professional Services Industry on the Rise

As cyber incidents continue to evolve in complexity and focus, we have been able to identify common trends for companies to consider. While the healthcare industry used to be the top cyber incident industry, according to Chubb data, the professional services industry is now the leader. Over the past four years, we have seen a 10% increase in Professional Services cyber incidents. It is important to note that Professional Services is largely an email driven profession, meaning there are many opportunities for employees to click on malicious links, driven by email phishing.

North America - Cyber Claim % by Industry



Chubb Insight – What Can Be Done?

As more people are working remotely, here are six ways to help protect your remote workforce against cyber threats:

1. **Make sure you have the necessary network bandwidth**, data storage, and computing power to meet the needs of the increase in traffic. Make certain your business can handle the number of employees working from home.

2. **Keep your systems up to date.** Make sure your software and applications are regularly updated and immediately patch any identified weaknesses.

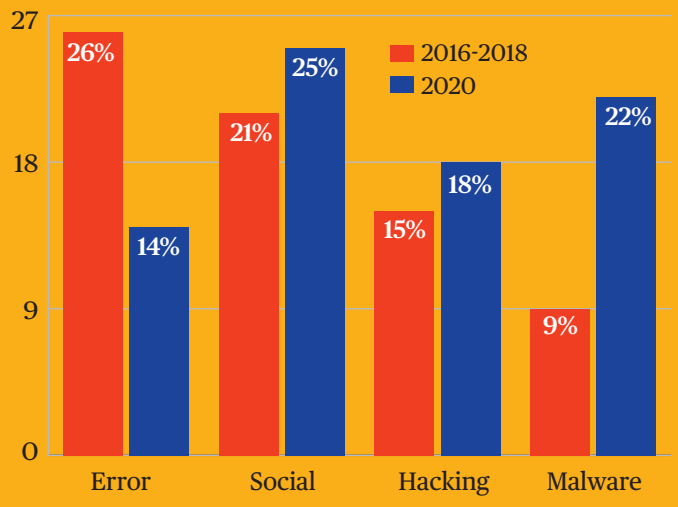
3. **Use a Virtual Private Network (VPN) when connecting to the Internet.** It will encrypt your activity so it can't be accessed by someone else.

4. **Always use strong passwords.** Don't designate the same password for multiple logins and consider using password management software, like Dashlane, to ensure that you are using unique, strong passwords for everything.

5. **Use Multifactor Authentication (MFA) on your accounts.** By requiring at least two authenticating factors to prove your identity before you can access protected data, you can thwart criminals attempting to enter private networks remotely.

6. **Avoid sending private information to a website or an unfamiliar email address.** Look carefully at web and email addresses. Criminals' websites often look similar to the ones you trust, and phishing emails are the most common way bad actors trick people into clicking on a suspicious link or attachment so they can access your personal information.

North America – Leading Causes of Cyber Claims



- Email Phishing still largest threat action
- Internal Actors dropping
  - 2017: 47%
  - 2020: 19%
- External Actors rising
  - 2017: 42%
  - 2020: 70%
- Attacks more malicious

Malware (Malicious Software) Exposures

We are seeing a decrease in error/misuse type incidents and a recent increase in exposures linked to malware, a malicious software. As malware incidents become more infectious, demands and costs associated with these incidents continue to rise. Over the last two years, malware-related incidents have accounted for 22% of our claims in 2020, compared to 25% for social, or email phishing, another leading cause of cyber claims. It is also important to note that many malware incidents initially arise from email phishing.

Most Cyber Risks Claims Are Coming from Outside the Company

Incidents caused by external actors, such as email phishing, business email compromise, and ransomware, are rising, while incidents arising from internal threats, such as when employees misuse information or make errors with protected information, are on the decline. Especially with email phishing, it is important for those working from home and employers who have remote workers to take additional care in protecting against cyber threats.

Bringing Cyber Risks to Life - Claims Scenarios

Professional services organization website hacked, data scrambled
When our client's service representatives noticed that member registration information on its online portal was incorrect and data had been scrambled, the professional services firm called Chubb. We engaged an incident response coach and a forensic services firm from our cyber panel to help. They determined that someone had hacked into the client's website and gained unauthorized access to their external web portal. The forensic firm found no evidence that Personally Identifiable Information was disclosed during the attack and only non-sensitive data had been breached.

Phishing emails compromise asset management firm
Our client, a global asset management company providing discretionary investment management for private clients, pensions, endowments, and family offices, discovered that one of its employee's email accounts had been compromised and phishing emails had been sent to four of his contacts, including three clients. Client information such as account numbers, account values, names, addresses, and possibly Social Security numbers had been compromised. The firm called Chubb, who brought in a forensics team and breach coach, and ordered credit monitoring.

To learn more about cyber trends, including the Chubb Cyber Index℠, please visit www.chubb.com/cyber.