# CYBER RISK

**by Steve (Ryan) R. Corbin, VTS Software Engineer**

## *Cyber attacks are in the news again, am I at risk?*

### INTRODUCTION

You may be tired of hearing it but data IS the currency of digital era. As with all forms of currency, Criminals want to steal it, Governments want to regulate it, and Businesses are having to learn to protect it. Cyber attacks are no longer only the concern of Cybersecurity professionals. Consumers are concerned with how their data is used and sold, while governments are beginning to regulate how businesses store and use data that they collect. This means that cyber risk is becoming more important when calculating business risk. The average attack costs $3.92 million, and regulators can assess fines without an attack taking place.[1] Like all risk Cyber risk has to be accepted, mitigated, and anticipated. Cyber risk effects both businesses and individuals, so while this article will discuss business networks the risk exists on home networks as well. Covid-19 has forced many industries to adopt work from home policies that connected employees home networks and business networks, increasing the attack area for cyber threats.

### THREAT ACTORS

Cyber risk can come from many sources, and businesses and individuals need to be aware of access points. Adversaries will exploit any access point to get a foothold into a network. Large sophisticated criminal organizations, novice hackers, Foreign governments, and even a businesses own employees have been involved in cyber attacks for personal gain.

External threats were the largest cyber threat in 2020. Accounting for 70% of incidents recorded in the Verizon Data Breach Investigation Report (DBIR).[2] External threats are individuals outside of the organization that seek to gain access to an organizations data. These threats can steal data, drop ransomware, take down systems, or modify data to defraud a business. Threat actors can be categorized in numerous ways, such as operational region, motivation, tactics, and notoriety. For this section I categorized the threat by tactic and motivation. This list can be a good starting point for some, but some industries may need to classify their threat into more specific categories to more effectively evaluate their overall risk.

**Advanced Persistent Threat (APT)**
APT organizations are capable adversaries who employ advanced intrusion techniques to gain access to a network and remain for an extended period of time.[3] These are often state-sponsored actors who may conduct espionage or criminal activity. APT30 is a suspected Chinese state-sponsored APT group that has been operating in the Southeast Asia region for over 10 years.[4] While APT organizations have targeted companies and individuals with direct links to government activity, they also target journalists and supply-chain companies that can be used as bridges into larger organizations.

**Cyber Criminals**
Cyber criminals include all threat actors who use technology to perform actions for financial gain. Cyber criminals who infiltrate networks usually employ smash-and-grab tactics rather than more sophisticated clandestine intrusion techniques. This can include ransomware, ransom-designed Denial of Service, data theft, and fraud. Cyber criminals can sell stolen

1 https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
2 https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/
3 https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats
4 https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
rcorbin@vtscyber.com
703.498.2150 703.498.2149

data, malicious tools, or access to networks over the dark web. The dark web is, simply, websites on the internet that are not indexed by search engines and require a special browser to access. Selling network access means that there may be a delay between network intrusion and the final attack.

**Hacktivists**
Hacktivists infiltrate a network to disrupt services or steal data that supports a cause. Anonymous is a well known hacktivist group that has carried out these types of activities. The activist threat is constantly changing and predicting how the groups objectives will change day-to-day is an exercise in futility. The morality and ethics of activism depend on an individuals own beliefs.

**Terrorists**
Terrorists are similar to hacktivists, in that they are both conducting the attack to support a specific cause. The difference between terrorism and activism is a disregard for the safety and well-being of people. A terrorist attack will often put people in danger, and may lead to deaths. It can also be an attack that is just associated with a terrorist organization.

**Inexperienced Hackers**
The Verizon 2020 DBIR identified that 3% of incidence/breaches reported were the result of inexperienced individuals who were learning to hack or hacking to build their reputation. This is a very low number of incidences. This group is comprised mostly of young individuals who are experimenting with hacking, and their target selection is very hard to predict.

Insider threats are actors that can harm a network and have legitimate authorization to operate on the network. This threat includes malicious insiders, human error, and unwitting employees. Training, security audits, and vigilant management are the best methods for mitigating this threat.

**Malicious Insider**
A malicious insider is an employee of the company who knowingly and willingly participates in a cyber attack. Misuse by authorized users accounted for only 8% of incidents in 2020, according to the Verizon DBIR.[5] While malicious insiders represent a very small number of incidences, they can be harder to identify and the impact can be magnitudes larger than other more frequent attacks.

**Human Error**
Human error is unavoidable, but makes up a large section of internal threat incidents. Misconfiguration of systems, access points, encryption, and security protocols can result in an open window for attackers, and misdelivery of email is literally handing data away. According to Verizons 2020 DBIR, errors were the cause of more incidents than social engineering and malware.

**Unwitting Employees**
While normally an unwitting participant of an external attack, every employee represents an exploitable path. The World Economic Forum predicts that permanent remote work will double in 2021[6], which could make their personal cyber security a liability for businesses. Hacking network end-points aren't the only paths for adversaries phishing, whaling, downloads, and social engineering can target almost any employee.

**Third Party Services**
Third party services are responsible for maintaining security on their platform that prevents adversaries from using their services as a vector for infiltrating your network. Recently, there have been two major events that have highlighted this

5 https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/
6 https://www.weforum.org/agenda/2020/10/permanent-remote-workers-pandemic-coronavirus-covid-19-work-home

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
rcorbin@vtscyber.com
703.498.2150 703.498.2149

threat in the news. One is the hacktivist attack on Parler, which the hackers claim was possible because Twilio, an American cloud communications platform that provided the platform with phone number verification services, revealed the services Parler was using for user-authentication.[7] Twilio insists that they are not responsible for the attack, because they weren't providing services at that time. However, the hackers were able to leverage the information about what services Parler used in order to gain access and escalate their privilege. Another example is the SolarWind supply chain attack that was able to corrupt the build server to use SolarWind as a delivery mechanism for their malware.[8] These two attacks highlight the dangers posed by third parties not just through the services they provide, but the information and insight they possess.

## TARGETS

The data targeted by threat actors can range from government secrets to a single email address, but some information has been shown to be more valuable than others.

### Credentials

Credentials are the most popular type of data stolen. This information can be used to take over accounts, gain access to restricted networks, used in brute force attacks, or credential stuffing attacks. 65% of people admit to reusing passwords across multiple sites and were responsible for 80% of breaches in 2019.[9] Digital Shadows reports there are over 15 billion credential pairs for sell on the dark web, with 5 billion unique pairs.[10] Financial account credentials, the most expensive at a set price, sell for around $70, while administrator account credentials are auctioned off to the highest bidder, up to $140,000. Even social media, media streaming, and adult-content site credentials can be sold on the dark web.

### Finance

Financial information is always a focused target of cyber criminals. Cyber criminals target credit card information, bank accounts, invoices, accounting credentials, and anything that can pay off quickly.

### Health Information

Healthcare facilities are more likely to pay ransoms due to the high cost of implementing security solutions across their entire network and the fines associated with regulations such as GDPR.[11] Health records are also valuable due to the amount of personal information they contain such as dates of birth, social security numbers, and credit card information. The average cost of a healthcare record on the dark web is $60. These records can be used to secure pharmaceuticals, create fraudulent insurance claims, and even be combined with additional records to create false identities.[12]

### Intellectual Property

Intellectual property (IP) can be proprietary products, trade secrets, customer lists, source code, or any other data unique to an individual business. This information is used to create counterfeit products without regard to health and manufacturing standards, and pirated digital products can provide an easy income stream for cyber criminals. Source code can also be used to develop malware and hacking products to assist criminals in gaining access to other networks. In some cases IP has resulted in development of technological advanced products in countries overseas who do not recognize IP rights.

### Defense Intelligence and technology

Defense Intelligence and technologies are often targets of state-sponsored APT organizations conducting cyber espionage. Industries operating in this area are required to implement specific cyber security frameworks and defenses in order

7 https://cybernews.com/news/70tb-of-parler-users-messages-videos-and-posts-leaked-by-security-researchers/
8 https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chain-attack/
9 https://www.idagent.com/blog/10-password-security-statistics-that-you-need-to-see-now/
10 https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover
11 https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/
12 https://secureops.com/data-breaches/healthcare-breaches/

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
rcorbin@vtscyber.com
703.498.2150 703.498.2149

mitigate the theft of sensitive information. While this data is usually secured well by manufacturing organization, third-party and supporting organizations are often targeted so that information can be pieced together.

**Operations**
While data is the major target of most cyber attacks, some attacks are executed to affect operations. Distributed Denial of Service (DDoS) attacks are meant to prevent access to an  organizations services. DDoS attacks can be used similar to ransomware, extorting an organization for money, or they can be used as a form of activism, such as the 2020 DDoS Anonymous attack after the death of George Floyd.

## SOLUTION

**Mitigate**
The best way to mitigate cyber risk is to mitigate attacks early. The National Institute of Science and Technology (NIST) has a Cybersecurity Framework that aligns with a Risk Management Framework (RMF) for cyber risk, and training is available to inform and certify personnel[13] in how to leverage this framework.

The Cybersecurity Framework[14] is a voluntary framework developed by NIST to guide organizations on Cybersecurity best practices. This framework is a collaboration of academia, industry, and the Federal Government made up of existing standards, guidelines and best practices. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, and Recover. Identifying threat actors, target data, and access points are a critical function. Examples of access points can be physical end-points and non-malicious insider threat actors.

The Risk Management Framework is a system to aid organizations in selecting and implementing a set of appropriate controls to manage Cybersecurity risk.

> *The Risk Management Framework provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.*[15]

The RMF is broken up into a series of steps that align with government and technical publications that provide additional information. Organizational policies are a major contributor risk management and set the tone for good or bad security practices throughout an organization. A favored policy, outlined by NIST 800-207, is a Zero Trust policy. Zero trust is an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.[16] This places a focus on securing the authentication process, website design, microservices, and cloud assets instead of focusing on traffic over the network.

## INSURE

Cyber insurance, sometimes called Cyber Liability or Cybersecurity insurance, is a product created to protect companies when the inevitable does occur. Cyber insurance is an insurance product that helps cover the recovery cost of a cyber attack. Cyber insurance often covers data recovery, forensic investigations, legal fees, and customer reparations.[17] Although, like any insurance, organizations should carefully read and understand what is covered in their individual policy.

13 https://vtscyber.com/training-certification/
14 https://www.nist.gov/cyberframework/new-framework
15 https://csrc.nist.gov/projects/risk-management/rmf-overview
16 https://csrc.nist.gov/publications/detail/sp/800-207/final
17 https://www.zdnet.com/article/what-is-cyber-insurance-everything-you-need-to-know-about-what-it-covers-and-how-it-works/

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
rcorbin@vtscyber.com
703.498.2150 703.498.2149

Some business policies may include some cyber-related coverage, and some coverage may come at a premium, such as Business Email Compromise or DDoS attacks.

## VIGILANCE

While the NIST Risk Management Framework is a voluntary guideline for businesses, organizations must remain vigilant. There are 3rd party services that offer risk management services. Many provide consultation, training, and security services based on proprietary, NIST, or other management frameworks. VTSCyber is one such company that offers assistance in navigating and conducting the risk management process following the NIST standard. Traditionally companies have managed risk through various proprietary software of spreadsheets manually, but with the advancements in AI, computing, and cybersecurity automated smart management platforms have been developed that can help organizations be more secure. Traditional methods such as Pentesting, security audits, and asset reviews are great at finding problems that currently exist, but good risk management can prevent a lot of problems before they start. CISA reports that 85% of targeted cyber attacks are preventable through keeping systems updated and patched.[18]

## CONCLUSION

Cyber risk should be a major consideration for any business in today's digital world. As remote work expands and businesses become more dependent on the internet and internal networks for conducting business, cyber crime expands in tandem. New solutions introduce new vulnerabilities, and sooner or later an attack will hit home. However, a digital presence is a necessity, so businesses will have to learn to accept some risk. A risk management framework tailored to cyber risk can ensure that the policies and practices a business uses mitigates risk instead of introducing new vulnerabilities. Cyber Insurance can protect a company financially when attacks occur, and risk monitoring services can make sure that emerging threats are mitigated before your network falls victim.



[18] https://us-cert.cisa.gov/ncas/alerts/TA15-119A

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
rcorbin@vtscyber.com
703.498.2150 703.498.2149