PUBLISHED OCTOBER 2023

Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

The American Academy of Actuaries is a 19,500-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policy makers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

© 2023 American Academy of Actuaries. All rights reserved.

Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies

Published October 2023

Introduction[1]

"Data breach," "hacking," and "cyberattack" are all common terms used consistently in the media, but mainly when they pertain to large organizations or household names' X (formerly Twitter) accounts. However, individuals who use cell phones, computers, or any digitally connected devices are subject to the same risks. Much like business entities, individuals can't completely negate these risks without living completely off the grid. Businesses and individuals can, however, take measures to help mitigate their risk from cyber-attacks. This document will help identify some of the penetration points of cyberattacks from an individual's perspective and examine how an individual can work to minimize their risk of being hacked.

Personal Cyber Risk Profile

Types of Personal Cyber Risks

Attackers can infiltrate or gain access to an individual's information in many ways. Some of the most common ways include:

- **Phishing schemes:** Attackers can create emails that look like they are from banks or lending institutions that ask for specific account information to gain access. One common scheme for people buying a home includes attempting to convince victims to wire their closing costs to attackers. Software such as ChatGPT could make drafting these emails easier for criminals to create phishing emails.
- **Social engineering:** Attackers can scour social media sites to find out personal information about potential victims. Attackers use this information to impersonate victims and extract trusted information from friends or family members. Attackers then use this information to gain access to victims' or victims' acquaintances' financial accounts or other sensitive information.

1 This document references a few specific products and services. The Academy does not recommend or encourage the use of any particular service, company, or product. They are referenced as examples of what may be available in the marketplace. Individuals interested in a particular type of service should thoroughly investigate various providers and products for comparison and determine which, if any, meet their needs.

- **Wi-Fi network hacking:** There are many tools available online that allow attackers to gain access to an individual's home Wi-Fi network. Once attackers have access to the home's network, they can access financial information and any other sensitive information the user may have on their computer.
- **Malware, spyware, and ransomware:** Through clicking a bad link on a website or in an email, a small piece of software can be installed on a user's computer or phone that can track everything that a user does on that device or take it over completely. In the case of ransomware, the user may have to pay attackers to be able to gain access again.

These are just some of the ways that attackers utilize to gain access to personal information, but this list is ever-evolving.

Personal vs. Commercial Risks

For the most part, the types of risks that individuals and companies are subject to are similar. Hackers may try to infiltrate an organization's network by sending a phishing email from the CEO requiring urgent action, or attackers may perform a brute force attack by using trial and error to guess a password and once in the network, they can cripple a company's whole network. Attackers may use a lot of the same methods to gain access to a business' network as they would to gain access to an individual's personal information. Once they have accessed an individual's network, the type of losses that can occur is generally similar between corporations and individuals. A recent paper published by the Society of Actuaries Research Institute[2] groups the risks associated with an attack on an individual's smart home system into the following categories:

- **Data breach:** Data breach risk is the exposure of personal private user data that can be collected from an individual from their electronic footprint and can be caused by exploitation of vulnerabilities in smart devices or malware attacks.
- **Loss of use:** Loss-of-use risk refers to the data recovery, repair to a device, and system restoration due to malware or denial-of-service (DoS) attacks.
- **Ransomware:** Ransomware risk refers to being locked out of your device until you pay a ransom.
- **Cyber extortion:** Cyber extortion occurs when there are threats to release an individual's private videos, photos, financial information, or activities for financial gain.
- **Online fraud:** This risk is the direct financial losses (stolen account funds, unauthorized use of banking or credit cards, phishing schemes, etc.) caused by cyberattacks.
- **Theft:** Theft is the loss incurred by cyberattacks on security systems. An example of this would be if the attacker unlocks a smart lock and steals items from an individual's home.

2 "Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure"; Society of Actuaries Research Institute; 2023.

Another type of potential risk for individuals that may be the result of being connected through social media or other means of cyber communication is cyberbullying. This type of attack does not involve hacking into an individual's devices or network, but rather this involves bullying someone via SMS, text, apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or malicious content about someone.[3]

While the size of loss in total dollar amount may not be comparable between individual and commercial cyberattacks, the impact to an individual may be higher and much longer-lasting. An individual could lose their whole life savings to a phishing scheme, but the same amount could have minimal effects for some companies.

With an increase in the number of employees working remotely, the line between personal and commercial cyber risks has become increasingly blurred. For example, if an individual is using a company-issued laptop but connected to their home router, the responsibility of loss could depend on how the attacker infiltrated the system. If someone hacks a home Wi-Fi network, the individual could be held responsible, but if the individual clicks on a suspicious link in their company email, the responsibility may lie with the employer(s).

Personal Cyber Risk Mitigation Strategies

While an individual may never completely eliminate all personal cyber risk, they can use many of the same mitigation tactics and strategies that businesses use to mitigate risk and protect themselves online.[4] For example, individuals can:

- Keep software up-to-date;
- Avoid opening suspicious emails;
- Keep hardware up-to-date;
- Use anti-virus and anti-malware software;
- Use a VPN to privatize their connections;
- Change passwords often and make them tough to crack; and
- Enable 2-factor authentication.

These are just some tips to make individuals more secure and help thwart cyberattacks. However, what if an individual's home network or computer is hacked? Are there products or services that may help in this scenario? There are two forms of protection that could assist: passive and reactive. One example of a reactive solution is a product that helps

3 "What Is Cyberbullying"; StopBullying.gov; Nov. 5, 2021.
4 "21 Cybersecurity Tips and Best Practices For Your Business"; Titanfile; 2021.

monitor an individual's credit score to determine whether their financial accounts have been hacked. These reactive solutions will alert the customer after an incident occurs and has already caused damage. Passive solutions constantly check your network for potential attacks or scour the dark web to tell if any data has been leaked or sold.

Both options work well for alerting an individual after their information has been stolen or the network has been attacked, but the drawback is that there may be direct financial consequences to victims. For example, victims will not be compensated for their financial loss and the consequences of their network being attacked.

The products and services mentioned above could serve as indicators of loss, and an insurance product could help provide protection should the individual experience a loss from an attack. For example, suspicious credit score activity reported by the credit monitoring applications may prompt the individual to take corrective actions that may require closing of accounts, opening new accounts, or recovering funds that have been spent on an individual's credit account. There are personal cyber insurance products currently available that will help an individual recoup these losses. For example, some insurers offer a personal cyber insurance product that offers protection against cyberbullying and cyberattacks, and these policies off financial assistance coverage for the reimbursement of funds that have been taken and are nonrecoverable. Individual cyber insurance products that cover cyberbullying will cover the costs of counseling, provide security measures to stop the bullying, and will sometimes protect you if your child is the one who is doing the bullying.[5]

Other insurers offer an endorsement to an individual's homeowners, renters, or condominium owners policy that will protect an insured against many of the same perils covered in stand-alone policies. Cyber endorsements can be added onto a policy for as little as $25 per year with limits up to $15,000. This coverage reimburses the insured for the costs associated with cyberattacks, cyber extortion, identity restoration case management services, contingent credit monitoring, and fraud loss coverage.[6]

5 "Cyberbullying Protection"; Chubb; 2023.
6 "Identity restoration insurance can help you recover"; State Farm; 2023.

Future of Personal Cyber Risks and Cyber Risk Insurance

While it is difficult to determine the number of cyberattacks that have impacted individuals, a blog post by Check Point Research states that the number of cyberattacks increased by 38% since last year—and with new and emerging technologies like ChatGPT, the number of attacks are predicted to rise.[7] Additionally, with the rise in the number of cyberattacks on organizations, the number of cyberattacks experienced by individuals is also expected to increase. There are many contributing factors to the rise in cyberattacks for individuals, but they all generally come down to the same idea: interconnectivity. Any time a digitally connected device (e.g., cell phones, smart home devices, self-driving vehicles and others) is used, the owner may be at risk. As technology advances, the world becomes increasingly connected.

Certain advances, while making life more convenient, also have the drawback of allowing attackers to gain easier access to important data. As discussed earlier, employees working from home have created an easier access point for would-be attackers.

Another convenience that comes at the price of the vulnerability is the widespread use of single sign-on (SSO) websites. Some websites now allow the user to use their social media credentials to create and log in to their site. *Wired*[8] addressed how the use of these SSO mechanisms allows for a single point of entry for potential attackers. Therefore, instead of having to crack several passwords, the attacker would only have to access the user's social media account to have access to all the user's information that are stored behind the SSO login credentials.

Currently, the amount of data pertaining to individual cyberattacks is limited; with the increased popularity of these types of coverages, the amount of data will grow. The current products offered as additions to an individual's homeowners or renters policy may be rated simply by applying an increased limits factor to a base rate. As the volume of data grows and the products develop and mature, insurers may be able to create more nuanced rating plans where risks may be more accurately priced.

7 "Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks"; Check Point; Jan. 5, 2023.
8 "Think Twice Before Using Facebook, Google, or Apple to Sign In Everywhere"; *Wired*; Sept. 21, 2020.

Conclusions

With the amount of information each individual stores on their phones, laptops, tablets, and other devices connected to the internet, it isn't feasible for someone to be able to eliminate their risks of being subject to a cyberattack, but there are some steps that an individual can take to help mitigate risk. Potential options to begin mitigating risk include choosing strong passwords or passphrases, changing your passwords regularly, and not duplicating passwords across multiple accounts.

Individuals should also be wary of suspicious emails and not click on links that could lead to harmful sites. As further means of protecting oneself from cyberattacks, an individual can also purchase a standalone cyber insurance policy or a cyber endorsement to their current homeowners/renters policy to help protect them from financial loss in the case of a cyberattack. These policies are generally affordable and can save an individual time and stress, and may help recoup funds if financial accounts are infiltrated.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

© 2023 American Academy of Actuaries. All rights reserved.