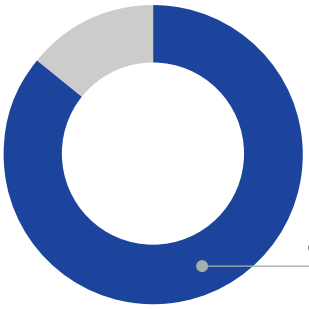
Chubb Cyber Risk Survey: Executive Summary

Personal Risk Services

Cyber Risks: Protecting the Online You

In an age of determined cyber criminals, even the smallest cyber attack can have real-world implications for individuals and families. To exacerbate the problem, these cyber criminals–buoyed by a rise in internet-connected devices and the proliferation of personal data as a commodity–are gaining new entry points to personally identifiable information every day. As a result, hacks, ransomware, phishing, and more are increasingly common and are having a greater impact on individuals and families than ever before.



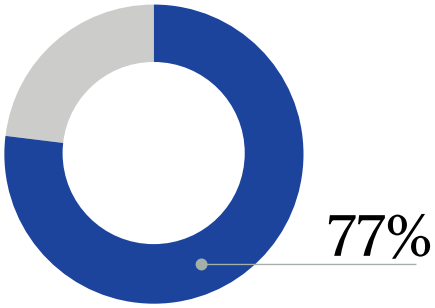
Percentage of respondents who report being "somewhat" or "very" concerned about a cyber breach.

Individuals are largely underprepared for these growing risks. The 2018 Chubb Cyber Survey found that most people either underestimate or are completely unaware of the common cyber threats that are targeting their personal information across social media sites and through devices ranging from personal laptops, smartphones and voice assistants, to smart refrigerators and thermostats.

While most (86%) are concerned about a breach on some level, inertia is preventing people from taking basic measures to protect themselves: only 30% regularly change passwords, 29% use multi-factor authentication to sign into accounts and just 40% have cyber security software such as malware protection installed.

They may unknowingly be putting their families at risk as well. While most adults (87%) implement some form of protection to their child's online activity, they do so based solely on age–a common misstep, as even older children and teenagers lack understanding when it comes to cyber safety. As younger generations become increasingly comfortable with what they share about themselves online–from vacation plans to major life events–individuals and families are further opened up to associated cyber risks.

For high-net-worth individuals and families, the stakes are even higher. As a segment, high-net-worth individuals are more likely than others to feel concerned about a cyber breach (86%) – and it makes sense. This group is more likely to be business owners or senior business executives with access to confidential client and employee information, proprietary intellectual property and other sensitive information that could spell disaster if stolen or leaked.



Percentage of respondents concerned about having credit card number stolen.

We have reached an age in which the digitization of data makes cyber crime one of the most pressing issues for individuals and businesses alike. According to the Insurance Information Institute, in 2017 alone, 16.7 million individuals were victims of identity fraud, accounting for $16.8 billion in stolen funds.

It's time to get smart, fight back and protect the online you. The 2018 Chubb Cyber Risk Survey examines what individuals are doing to protect themselves online–and where the gaps still exist. Read on for a complete account of survey findings and to learn how individuals can stay safe in a world where there's a new cyber threat emerging daily.

Section 1: People Don't Know What They Don't Know

Knowledge is power–and true to this, most people feel powerless when it comes to cyber safety. While seemingly weekly headlines about a new hack or data breach have certainly heightened awareness of cyber risks, there is a clear knowledge gap on the part of most people when it comes to understanding key cyber threats, as well as which data is most valuable.

Eighty-six percent of all respondents reported being "somewhat" (44%) or "very" (42%) concerned about a cyber breach. High-net-worth individuals were even more anxious, with 56% saying they felt "very" concerned.

And yet, what is most alarming is that many people have a misplaced sense of which type of personal data is most harmful to have stolen. Respondents placed too much concern on certain data being compromised, but demonstrated a startling lack of concern when it came to data that is actually more valuable if breached.

For example, bank breaches and other financial accounts becoming compromised were the top concerns (80%); however, the vast majority of banks and financial institutions will reimburse for lost funds in the event of a breach. Additionally, 77% of people were concerned about having their credit card number stolen, despite most companies having built-in fraud protections and relatively simple cancellation and replacement processes.

On the other hand, there is a lack of recognition that other personally identifiable information becoming compromised could be much more problematic. For example, obtaining a social security number is like hitting the data jackpot for a cyber criminal. In this vein, people seem to be unaware; less than two thirds (60%) of individuals said they were concerned about family members'

Frankenstein's Monster of ID Theft

Dr. Frankenstein's Monster was a fusion of parts that created something much larger and more powerful–though not quite as authentic as the real thing.

Cyber criminals use the same technique–gathering bits and pieces of your personal data–to create a rough copy of your online presence that they can use to open up accounts in your name, pretend to be you in online transactions, or even masquerade as you on social media to your friends, family and colleagues.

Because of this, it's important to be selective about where you give out personal information and the types of information you distribute, as well as have a clear understanding about which information in the wrong hands poses the greatest risk.

At the end of the day, most financial institutions (including credit card companies and banks) have restitution measures in place to make you whole. So, while breaches that expose smaller bits and pieces of your identity may seem less concerning, they are the tools hackers use to piece together a complete picture and access more sensitive information.

Children & Social Media Having "The Talk" (No, Not That Talk)

Most people **87%** say that they apply some form of online protections to their kids' online activity, most commonly stating that age is the major factor in deciding how to monitor activity.

37% say they do not allow children to use social media until they reach a certain age, and a quarter (23%) do not allow children under 18 years old to use social media at all. A third of respondents (34%) opt to activate child protection settings on devices as applicable.

However, staying cyber-safe online is age-agnostic. Parents should place less emphasis on age and more on how cyber-savvy their child is. A young tween who knows what red flags to look out for is less of an online liability than a college student who opens links inside every email they receive.

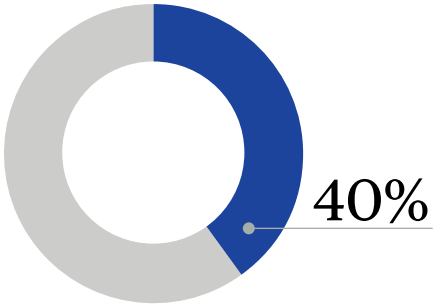
social security numbers becoming compromised, and only 16% are concerned about their children's information being compromised–even though accounts opened in a child's name can often go years without being detected. Medical records are also a valuable tool in the wrong hands, and just 30% reported being concerned about having this information breached.

Email addresses (18%) and proprietary business information (11%) are other overlooked data that could be devastating to lose. And while most people are not worried about their email address being compromised, there is a clear disconnect, as email exposures lead the way when it comes to perceived top threats (19%), ahead of credit agency breaches (18%) and company hacks (16%).

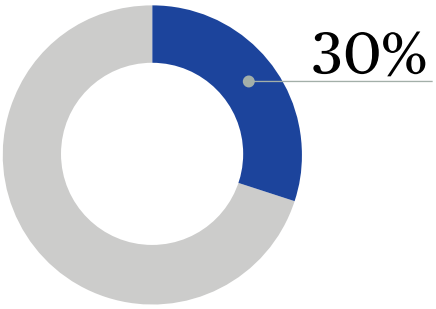
Other key threats that are overlooked include public WiFi exposures (12%), smart-home connected devices (4%) and unintentional human error (4%) all of which pose serious risk to individuals.

Furthermore, many people aren't sure exactly what it is that they're afraid of. Almost half (44%) of respondents were unable to correctly define the "dark web"–the private networks used by many online criminals to buy and sell illicit data–with one-in-five believing it to be a cyber attack itself.

Ransomware, the malware that restricts access to data until a ransom is paid, often in cryptocurrencies, is one of the most impactful threats in recent years. However, 50% of respondents defined it incorrectly, with one-fifth (19%) having never heard of the term. While the majority of respondents (65%) correctly identified phishing as an attempt to solicit personal information via email, just 25% were able to define brute force attacks, the trial-and-error process with which hackers attempt to gain access to a personal account, with 16% believing it involved a physical break-in to a storage or warehouse facility.



Percentage of respondents who use cyber security software–one of the simplest forms of online protection.



Bad password hygiene–only one-third say they regularly change online passwords.

Section 2: Giving Lip Service to Cyber Security

There are measures individuals can take to reduce some of their cyber risks. Given this, there is a massive opportunity for people to be better at safeguarding their personal information and data. While there is an awareness of the cyber risks associated with having an online presence, there is a pervasive relaxed nature when it comes to individuals' approaches to cyber security. People tend to know what to do, but now need to take the next step and act upon this knowledge.

For example, while respondents cited a credit agency hack as a top perceived threat–understandably, considering events of the past 12 months–just half of respondents regularly check their credit. Further, two-in-five respondents don't take the steps to regularly monitor their financial statements for suspicious transactions (61%) or delete emails from unknown sources (59%).

From there, it gets worse. Just 40% of respondents use cyber security software–one of the simplest forms of online protection. Less than one-third regularly change online passwords (30%) and use multi-factor authentication–a very simple yet effective tool–to log into their accounts (29%).

Password maintenance is another common area in which respondents overlook security. Bad password hygiene is rampant–only one-third (30%) say they regularly change online passwords, and 67% say they "always" or "often" use the same password for multiple online sites. More than half (54%) have shared one or more account passwords with someone other than an account holder. Two-in-five respondents (41%) don't even have their home WiFi network password protected, and of those who do have passwords, just 15% change them on a regular basis.

More Money, More Problems

High-net-worth individuals are more likely than any other financial class to express feeling concerned about a cyber breach (86%).

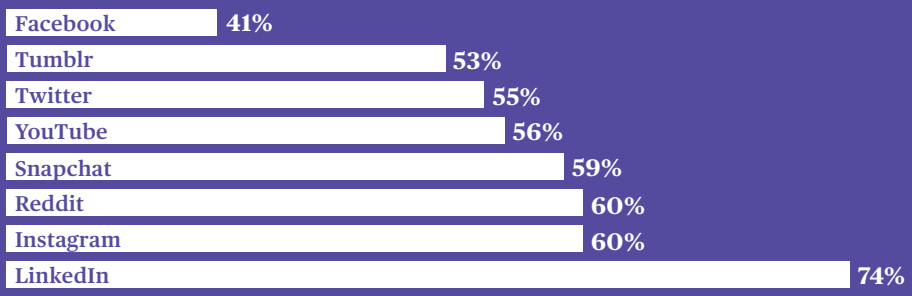
It is these same individuals who are most likely to use services such as family offices, trust and estate attorneys, art advisors and specialized doctors–service providers who may or may not implement the cyber security measures referenced above on their own accounts, or those of their clients.

For a high-net-worth individual or family with multiple accounts with extremely sensitive data being housed by multiple intermediaries, making sure that your partners and advisors are being careful with your data is a must.

It is important for advisors, consultants, agents and brokers to be aware of these concerns and understand how to keep their clients' data safe and secure.

Getting Too Social

Are individuals putting too much trust in social media to keep their information safe?



When asked about the perceived security of top social media sites, Facebook was at the bottom of the list, with just 41% saying that it was either somewhat or very secure, compared to Tumblr (53%), Twitter (55%), YouTube (56%), Snapchat (59%), Reddit (60%), Instagram (60%), and LinkedIn (74%).

However, the perceptions of respondents seemingly didn't affect their actions: despite being named the least secure, Facebook was by far the most highly-used, with 68% of respondents on the platform, compared to YouTube in second place at 51% and Instagram in third at 42%.

As trust in many social media outlets has eroded–rightly or wrongly–there's still a need for trustworthy education around cyber security and data security risks. Businesses can play a vital role in cyber security training and education, in both the professional and personal lives of their employees. However, just 20% of respondents say that they learn about cyber security from their workplace–less than online sources (38%), friends/family (36%) and the mainstream media (32%).

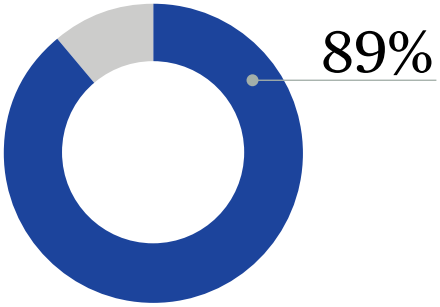
Section 3: Cyber Security at Work–Employers Should Lead the Way

When it comes to individuals' cyber habits in the home, there is a disconnect between the understanding of different cyber risks and the actions taken to protect against those same risks. There is a similar detachment at work as well.

Three quarters (75%) of respondents say their company has implemented "excellent" or "good" cyber security practices. However, Chubb's commercial claims data shows that there has been a 930% increase in the number of cyber insurance claims over the past 10 years–suggesting that even as companies establish better safeguards, there are still significant threat activities that continue to exploit the remaining vulnerabilities. This is also indicative of cyber criminals becoming increasingly sophisticated in breaching company systems.

In practice, while most employers do a good job putting the right measures in place to protect themselves and their employees, they could be doing even more to guard against long-term cyber threats. Businesses show that they are good at adopting certain cyber security tools, like firewall protection (59%), antivirus software (56%) and email spam filters (54%). Half say they practice good password hygiene. However, regularly updating operating systems (46%) and filtering for online content (40%) needs improvement.

Luckily, employees seem to understand the importance of strong cyber security in the workplace. Nearly all (93%) agree that they understand the intent of the cyber security measures their company has implemented and think the cyber security



The majority of respondents find complying with their company's cyber security policies to be simple.

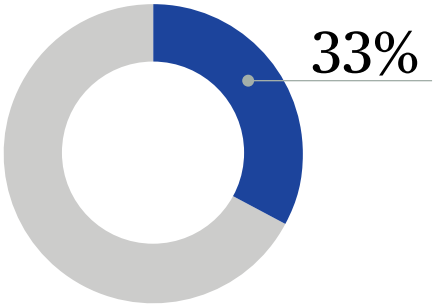
policies and precautions their company has implemented are reasonable (97%). The majority (89%) also find complying with their company's cyber security policies to be simple.

However, just 33% say their employers hold annual company-wide trainings or updates. While the policies themselves may be simple, with the continually evolving nature of cyber risks, an annual (or, preferably, more frequent) training on the latest risks and tactics of cyber criminals is necessary.

A Call to (Cyber) Arms

While awareness of cyber risks are on the rise–and people are beginning to move in the right direction when it comes to taking protective measures–society has not yet achieved a strong culture of cyber security. Many risks are overlooked, and there is a knowledge gap and lack of this type of specific cyber-education. This is becoming apparent at a hyper-critical time, as ever-greater amounts of data are stored online and on an array of devices, and as the Internet of Things continues to evolve. More data in more places simply serves to give cyber criminals more targets to aim at.

While proactive measures of cyber security are essential, in order to truly safeguard against cyber risk, a back-up plan is necessary. The best back-up plan is cyber insurance–with the best policies providing a mix of defensive protective measures along with fast response capabilities in a worst-case scenario. A good cyber insurance policy is more than just a financial loss mitigation tool–it can help individuals stay protected and prepared before a potential cyber attack, and also provide peace of mind knowing that you have a team on your side in the event one occurs.



Percentage of respondents say their employers hold annual company-wide trainings or updates.

Out of Office

Imagine this: You own a small, but quickly growing, consulting company. You're giving a talk at a conference and, during a break in the sessions, you log into your work computer on what you believe is the conference center Wi-Fi network.

The screen suddenly freezes. A message pops up telling you that your files have been encrypted and that you can only access them by sending $1,000 worth of Bitcoin to an IP address. You've become the victim of a ransomware attack.

Those compromised files include confidential client information, and you are worried that not only is your source of income now vulnerable, but you fear legal issues brought by your clients for failing to keep their information secure.

What do you do? Do you pay the ransom? How do you respond in the event of a lawsuit?

For many small business owners, entrepreneurs, or business executives, this scenario is more common than you might think, and can cause severe financial, reputational and legal costs. With the average cost of a cyber breach reaching more than $400,000, based on Chubb commercial claims data, the price can be steep.

To learn more about cyber and how Chubb can help individuals and families stay safe, please visit: Chubb's "Online You, Protected" Cyber Resource Center.

Methodology:

- This is the second survey by Chubb measuring consumers' approaches and behaviors toward cyber risk. Conducted by Research Now SSI, a leading global provider of first-party consumer and professional data, the online survey was fielded between June 6-13, 2018. The results are based on 1,204 completed surveys. A breakdown of respondents is as follows:
- Gender: Male (42%), Female (58%)
- Age: 18-34 (27%), 35-54 (40%), 55+ (33%)
- Regions: Midwest (20%), Northeast (23%), West (25%), South (32%)
- Socioeconomic Status: Middle Class (25%), Upper Middle Class (25%), Mass Affluent (25%), High-Net-Worth (25%)

Chubb. Insured.℠