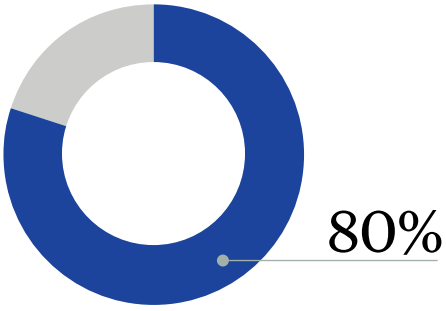
Chubb Cyber Risk Survey 2019 Executive Summary

Personal Risk Services

Online You, Protected: Third Annual Report

Top Line Summary Points

- While individuals say they understand their exposure, most don't recognize the source of their vulnerability
- Bad cyber behavior persists, with financially successful individuals as the most vulnerable
- Businesses continue to be vulnerable to cyber risk, largely due to a lack of employee education



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

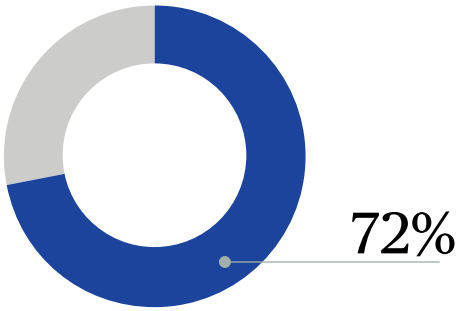
The emergence of new technologies could be considered a double-edged sword. On one side, it has driven new conveniences, including facial-recognition software that opens smartphones with ease and internet-connected capabilities that store passwords. On the other, those same conveniences have made criminal cyber incidents increasingly common. In turn, attacks now involve a multitude of different methods, giving cyber criminals new entry points into personal information and thereby having a greater likelihood of a detrimental impact on individuals and families more than ever before.

Despite the ubiquity of cyberattacks, the 2019 Chubb Cyber Risk Survey found that a majority of individuals continue to underestimate the most common cyber threats. In addition, Chubb's Third Annual Cyber Report, which examined individuals' comprehension of cyber risks, the steps they are taking to protect themselves, and where any gaps still exist, found the following:

While individuals say they understand their exposure, most don't recognize the source of their vulnerability
While a vast majority of respondents (80%) report being "somewhat" or "very" concerned about a cyber breach, these concerns have not yet translated into actions–only 41% of respondents have cybersecurity software (such as malware protection) installed on their devices, just 31% report regularly changing online passwords, and a mere 30% say they use multi-factor authentication to sign into accounts.

Bad cyber behavior persists, with financially successful individuals as the most vulnerable
Among populations, successful individuals are particularly vulnerable. For instance, 52% of successful individuals report being "very concerned" about a cyber breach, as compared to only 42% of mass affluent individuals, 33% of upper middle-class individuals, and 30% of middle-class individuals. Driving this concern is the fact that successful individuals are more likely to have access to confidential information, proprietary intellectual property, or other sensitive data that could be damaging–financially or reputationally– if stolen or leaked.

For the broader population, this does not mean they are in the clear. In fact, many might even be putting their families at risk. Chubb's 2018 Cyber Survey found that 87% of adults implemented some



Percentage of adults who implement the same level of protection as their child's online activity.

form of protection over their child's online activity. However, this year's survey found that just 72% of adults implement these same protections for themselves. Potentially more concerning is that most parents continue to base these restrictions on age—a common mistake, as they tend to focus more on age-appropriate content than cybersecurity. However, older children and teenagers often lack adequate comprehension of cyber safety.

Businesses continue to be vulnerable to cyber risk, largely due to a lack of employee education

Businesses aren't immune to cyber threats either. Just like individuals, companies are also trying to stay ahead of ever-changing cyber risks. The interconnection between networks and devices within a business' ecosystem means that company cybersecurity protections heavily rely on proper employee education and action. However, only 31% of respondents report that their companies provide them with annual company-wide trainings or updates. If proper employee education programs are not implemented, there may be longstanding business ramifications.

Additional information and further details from Chubb's 2019 Cyber Report follow.

Section 1: Awareness Desired, Action Needed

According to the study, most individuals (80%) are concerned about a cyber breach, but there remains a clear knowledge gap when it comes to understanding which data is most irreplaceable. For example, three-quarters (78%) of respondents were concerned about their financial accounts becoming compromised, despite the fact that most financial institutions will reimburse lost funds.

On the other hand, medical records that fall into the wrong hands can be costly and dangerous, yet just 27% of respondents report being concerned about having this information breached. Particularly troubling is that healthcare breaches are not isolated occurrences. According to the Chubb Cyber Index℠, cyberattacks in the healthcare industry have increased 1,800% since 2009. Taken together, this means that even if individuals make an effort to protect their information, it remains vulnerable due to poor institutional cyber practices.

Hackers are also thinking about the big picture when it comes to identity theft, and they are experts at piecing puzzles together. Therefore, email addresses—an item of concern to just 18% of respondents—are an underestimated source of exposure. Used in conjunction with other information scraped from the web, bad actors can just as effectively carry out a cyber attack.

Think this couldn't happen to you? Just ask Jane. After visiting her doctor for a routine annual check-up, she was notified several months later that her information was compromised when the provider's network was breached. Fortunately, the provider noted that no sensitive health or financial information was compromised, just her email and patient portal log-in password.

Less fortunate for Jane was the fact that the thief behind the hack was savvy. If Jane used her password for one site, wouldn't she likely use it for another? Bingo! The hacker was able to access Jane's social media accounts, where he

1,800%

cyberattacks in the healthcare industry have increased since 2009, according to the Chubb Cyber Index℠.

How Well Do You Know Your Social Media Friends?

24% say very secure

22% say very secure

21% say very secure

20% say very secure

15% of respondents say very secure

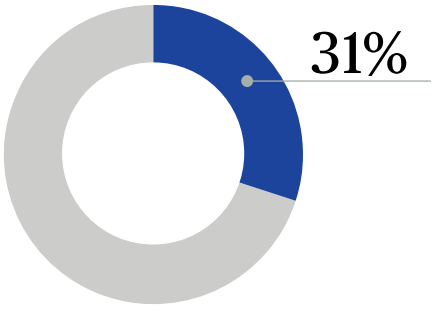
tracked down her birthday, spouse's name, and employment information. By putting these pieces together, the hacker eventually targeted Jane's bank account, swindling away thousands of dollars. While Jane ultimately recovered her lost finances, this is an all-too-common scenario.

Despite the fact that three quarters of respondents do not consider social media sites to be secure, many continue to knowingly share personal details and intimate information with these digital communities. When asked about the perceived security of top social media sites, none were considered "very secure" by a majority of individuals. Yet, respondents report that they frequently post personal photos of pets (37%), children (36%), and spouses (32%), as well as travel plans and photos (32%) to their social media channels.

Of that content, individuals most enjoy seeing baby photos (45%), travel photos (43%), and personal achievements (38%) in their feed. But just because they post it, does not mean that "friends" like it. Political posts were ranked as the most annoying content (62%), followed by photos of food (39%), and breaking news-style information (37%).

While individuals question the security of social media, they choose to push aside these concerns and continue to post personal information. In fact, half of survey respondents believe that they are "good" or "great" at finding personal information about others online. Furthermore, a worrying 76% of respondents felt that it was either "somewhat" or "very easy" for others to find information about themselves online. If a casual social media user can obtain personal information about a friend or acquaintance, imagine what a professional hacker can do.

Aside from cyber stalking, there are other malicious dangers lurking within the internet, including cyber bullying–identified by 82% of respondents as a major concern. This problem is real. The National Crime Prevention Council reports that nearly 43% of children have been bullied online and that one in four has had reoccurring experiences. This is an urgent online crisis that users can't continue to overlook.

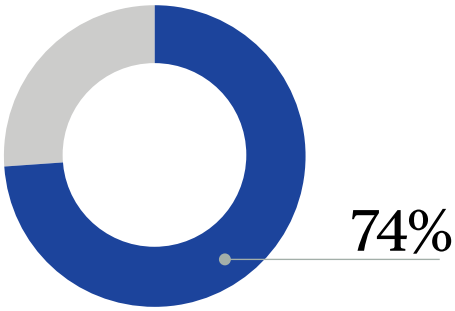


Only one-third of respondents report that they regularly change online passwords.

Section 2: One Cyber Step Forward, Many Still to Go

According to the survey, while individuals exercise certain cybersecurity best practices, there continues to be a lack of understanding about the sources of exposure. For example, while a majority of respondents regularly monitor their financial statements for suspicious transactions (59%) or delete emails from unknown sources (60%), only 41% of respondents use cybersecurity software–one of the simplest forms of online protection.

According to the study, password maintenance is another common area in which respondents overlook security. Specifically, only one-third (31%) of respondents report that they regularly change online passwords, and half (49%) have shared one or more account passwords with someone else. Of concern is that each of these statistics have remained consistent from 2018 to 2019, indicating a disconnect between knowing about and acting on cybersecurity best practices.



Percentage of individuals over 55 who regularly monitor their financial statements.

When examined by age, the study found that a consistently larger portion of older respondents employ better cyber practices than younger generations. For example:

- Seventy-seven percent of individuals over 55 delete suspicious emails, compared to half (55%) of respondents between 35 to 54, and just a third (36%) of respondents from 18 to 34.
- Three quarters (74%) of respondents over 55 regularly monitor their financial statements, whereas only half (57%) of individuals age 35 to 54 and just 33% of individuals 18 to 34 follow the same habit.
- Fifty-three percent of respondents over 55 are enrolled in a cybersecurity monitoring service. But, this same service is used by only 41% of respondents between 35 to 54 and just 29% of respondents between 18 to 34.

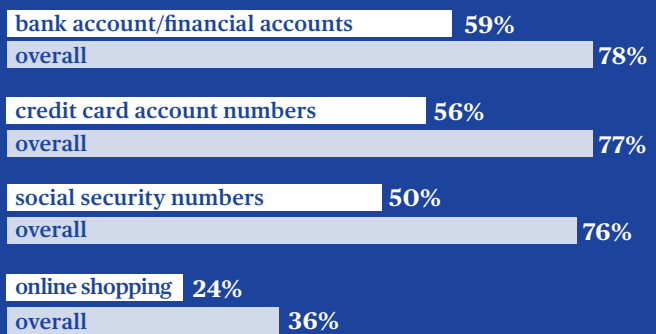
In most narratives, it's the younger generation teaching older generations about the latest internet trends. When it comes to cyber safety, however, it's clear that the tables have turned. The first lesson older generations should impart? The importance of talking with an independent agent and broker about coverage for a cyber-related incident. Without it, and in the event of a hack or breach which leads to a financial loss, individuals could be left without a safety net in place. In some cases, policies will also cover incident response expenses, including legal services, reputation management, and mental and emotional pain diagnosed by a physician.

What Really Matters to Successful Individuals

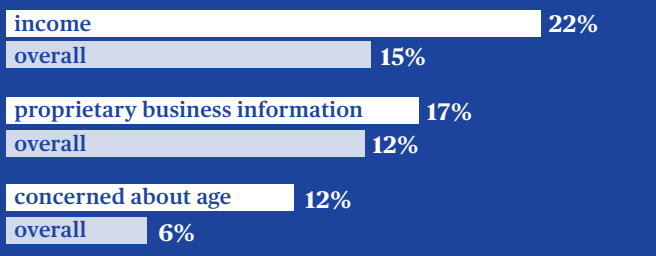
Eighty percent of successful individuals are "concerned" about a cyber breach, and 52% report that they are "very concerned." However, despite this worry, a significantly smaller proportion of successful individuals practice basic cybersecurity precautions as compared to other income groups. Consider that only 43% of successful individuals report that they delete suspicious emails, versus 66% of middle-class and 71% of upper middle-class individuals.

So, what are they worried about and how do their concerns compare to others?

As it turns out, successful individuals are less concerned about transactional information than the average respondent:



They are, however, more concerned about reputational information than the average respondent:



Outside of these reputational concerns, successful individuals also place higher premiums on protecting their social media accounts (26% vs. overall of 18%), travel accounts (16% vs. overall of 10%), and entertainment streaming accounts (14% vs. overall of 7%).

Moreover, successful individuals are also more likely to use attorneys, accountants, and advisors—and may potentially even outsource their cybersecurity protections. In turn, successful individuals were more likely to identify rogue trusted advisors, such as financial planners, accountants, and attorneys (16% vs. overall of 11%) as potential sources of cyber risk. Simply, the more partners involved, the more potential access points to sensitive data.

The bit of good news; however, is that successful individuals are more likely to purchase comprehensive cyber insurance than their peers (19% vs. 9% average). In the event of a breach, this is the one of the best ways to contain the risk.

1,215%
increase in the number of commercial cyber insurance claims over the past 10 years, according to the Chubb Cyber Index℠ claims data.

Section 3: Employer Employee Disconnect

The Chubb Cyber Index℠ claims data shows that there has been a 1,215% increase in the number of commercial cyber insurance claims over the past 10 years. This suggests that, even as companies establish better safeguards, significant threats remain.

Employee education lies at the heart of the problem. Rick, an employee on the accounting team at a small manufacturer in the Midwest, exemplifies the challenge. While the study found that 70% of respondents report that their company has "excellent" or "good" cybersecurity practices, only 31% of respondents—many of whom are just like Rick—report that their employer provides them with annual company-wide trainings or updates.

Why does this matter? In addition to just 19% of respondents who report that they learn about cybersecurity protections through their employer, more than a third say they most often learn about how to protect against cybersecurity risks from mainstream media (35%), and family and friends (34%). As a result, employers are left with a workforce that is unprepared to protect their business.

In turn, this education gap means employees and individuals cannot spot incoming attacks. According to the survey, while 54% of respondents correctly defined ransomware—a form of malware that restricts access to files unless a ransom is paid—this was the only common form of attack that a majority of individuals could correctly identify.

Most surveyed did not know the definition of, or had not heard of the following:

- 59% could not identify credential stuffing, an attack by cyber criminals to programmatically target a single online user using an email address and multiple password attempts.
- 72% could not identify Emotet, a type of malware which is designed to steal financial information and online banking credentials.
- 74% could not identify Ryuk, a new strain of ransomware that infects the victim's main computer systems and hides itself as a legitimate VPN user.

In the case of Rick's employer, this lack of cyber education resulted in a credential stuffing attack that led to significant financial harm. Because employees were not trained on the most common red flags associated with a phishing email—spelling mistakes, being sent at odd hours, and a return email address that does not match the sender's address (just to name a few)—employees were unable to spot the difference between a legitimate and fraudulent email. This meant that when Rick and his colleagues in the accounting team were targeted by a phishing email supposedly from their bank asking them to update their account information online, they complied. As a result, hackers were able to access login and password information that gave them access to their employer's bank account.

As cyber criminals become increasingly sophisticated in their efforts to breach company systems, a general understanding of these common attacks—and how they are enacted—can be extremely valuable. By requiring employees to undergo annual trainings, much of which can be conducted online and limited to an hour, employees may be able to identify breach warning signs before they become full-blown attacks—allowing companies time to potentially intervene before significant losses occur.

For companies looking for a training partner, talk with your insurance carrier as many have relationships with vendors.

The Time to Act is Now

While individuals are increasingly familiar with cyber vulnerabilities, there is still more that can be done. From 2018 to 2019, this report found ample evidence that not enough progress has been made in terms of implementing cyber risk protections. Many critical exposures continue to be overlooked, and there is still an overwhelming lack of cyber-specific educational programs—programs that are critical to closing the education/implementation gap.

While proactive measures are essential, a back-up plan is required to truly safeguard against any cyber risk. The best supplemental safeguard is cyber insurance—one that provides an inclusive mix of defensive and protective measures, along with fast response capabilities in a worst-case scenario. A good cyber insurance policy also includes more than just a financial loss mitigation tool: it can help individuals understand how to prepare ahead of a potential cyber attack.

To learn more about cyber and how Chubb can help individuals and families stay safe, please visit: Chubb.com/online-you-protected

Methodology:

This is the third survey by Chubb measuring consumers' approaches and behaviors toward cyber risk. Conducted by Dynata, a leading global provider of first-party consumer and professional data, the online survey was fielded between May 7, - May 17, 2019. The results are based on 1,223 completed surveys. A breakdown of respondents is as follows:

- **Gender:**
  - Male (46%)
  - Female (54%)
- **Age:**
  - 18-34 (21%)
  - 35-54 (40%)
  - 55+ (39%)
- **Regions:**
  - Midwest (22%)
  - Northeast (20%)
  - West (23%)
  - South (36%)
- **Socioeconomic Status:**
  - Middle Class (25%)
  - Upper Middle Class (25%)
  - Mass Affluent (27%)
  - Successful (22%)

Chubb. Insured.℠