Top Risks for Private Companies in the U.S.

Highlights from Chubb's Private Company Risk Survey

CHUBB®

Contents

Why Are Private Companies at Risk?

Leigh Anne Sherman
Executive Vice President
North America
Financial Lines

In past years, Chubb's Private Company Risk Surveys have focused on the liability risks and potential losses of lawsuits and fines, cyber theft and other commercial crimes – all potential risks that private companies should take steps to mitigate.

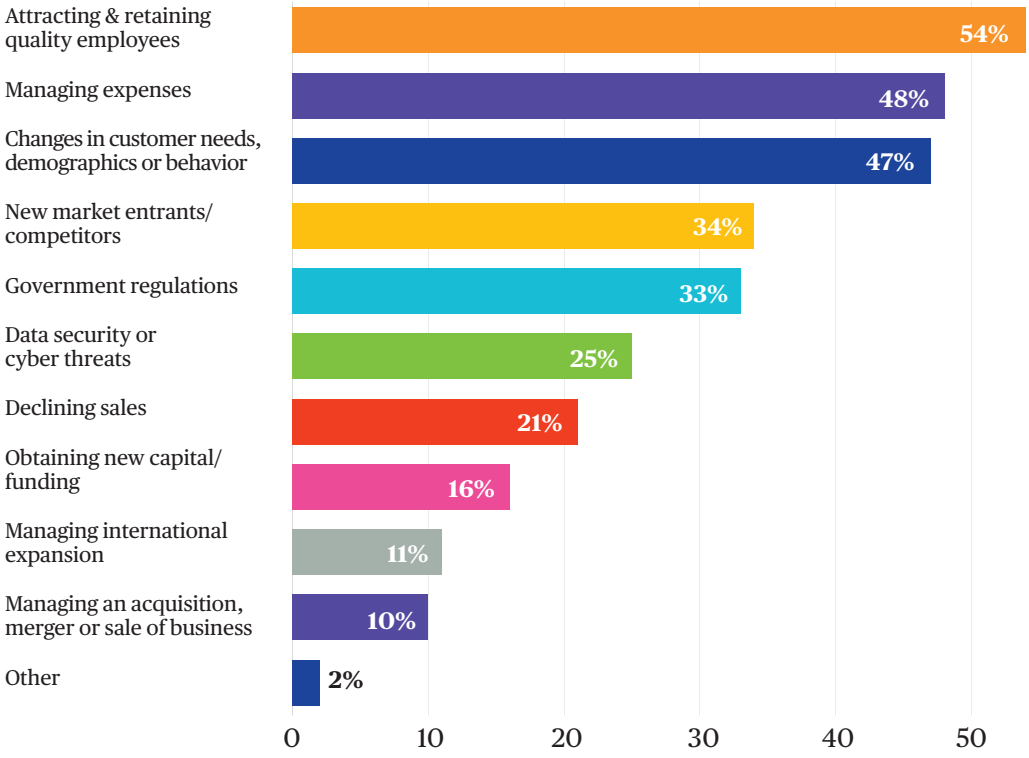
Our most recent survey also shed light on an additional risk that is often overlooked: the fact that such costly events inevitably take executives away from their primary responsibility of running the business. This hidden cost occurring in the aftermath of a loss event can be difficult to measure in purely financial terms. It can result in delayed initiatives, lost productivity, and an overall decline in the functional efficiency of the organization. The type of business under attack will determine the actual bottom line cost, but the time that key leaders may spend dealing with the fallout from an event is a real and inevitable feature of the private company landscape.

Despite compelling evidence that loss events can have devastating effects on a private company's operations, the latest survey reveals that three-fourths of all respondents remain unconcerned about the risk of potential damage…and none of those surveyed are concerned about all of their areas of exposure. Of those who do express concern, a majority are focused on just two areas alone: wrongful termination suits and cyber breaches. Given the range of risks that private companies may face, this finding seems quite worrisome.

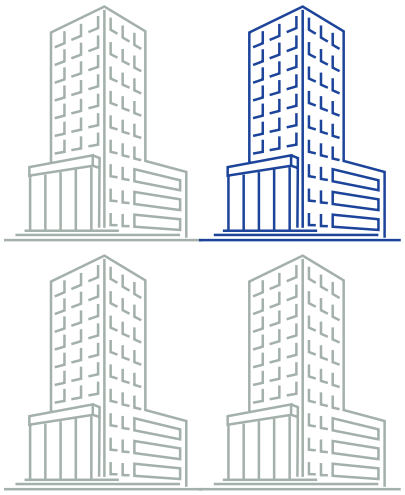
Fortunately, Chubb's most recent Private Company Survey offers a complete picture of the risks private company executives face, which may assist them in making wise decisions in the areas of Directors & Officers (D&O) liability, Employment Practices Liability (EPL), cyber liability, and commercial criminal liability insurance.

A Sampling of Key Findings

Top challenges anticipated by private companies in the next three years:



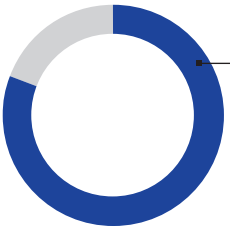
Less than one quarter of respondents are very concerned about potential damage to their company.



Of those who are, most are concerned with the possibility of a cyber breach or wrongful termination suit:

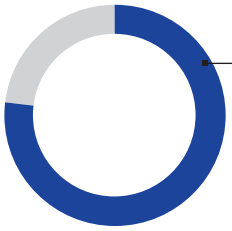
59%	Lawsuit for wrongful termination/discrimination/ harassment/retaliation
57%	Cyber breach or privacy loss involving non-public information
54%	Lawsuit for negligence in providing services to clients
56%	Employee theft of corporate or customer assets
49%	Workplace violence incident

Participating companies currently have the following risk management practices in place:



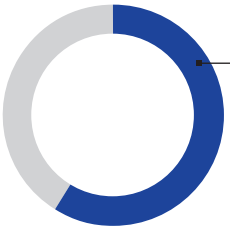
81%

Provide written HR policies banning employment discrimination and sexual harassment



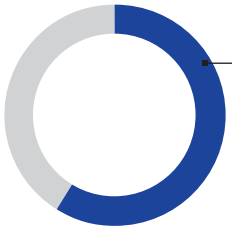
77%

Have a network security and privacy policy



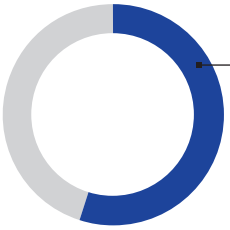
59%

Require mandatory training for employees on employment discrimination, sexual harassment or retaliation



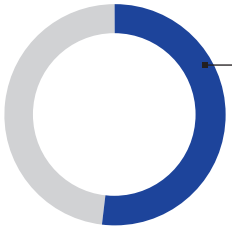
59%

Have a written business continuity plan



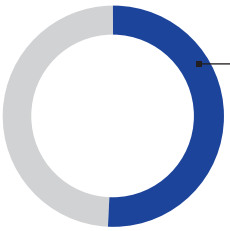
55%

Have a written policy addressing social media in the workplace



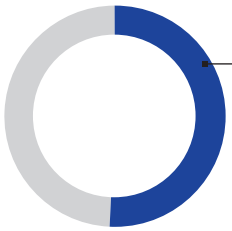
52%

Have a written corporate governance program



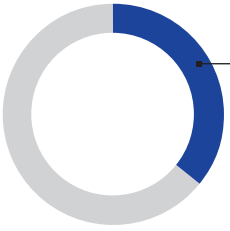
51%

Have a succession plan or perpetuation plan



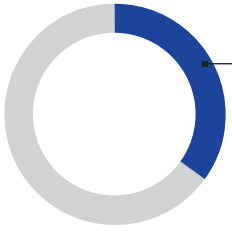
51%

Have procedures to avoid potential breaches of fiduciary duty



36%

Have an incident response plan for cyber breach or privacy loss



35%

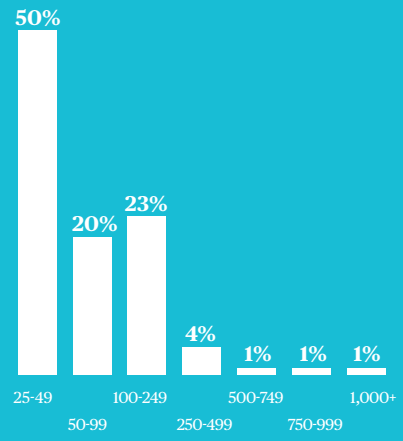
Have a specific risk management committee

Respondent Profile

27 years

Average length of time company has been in business

Average number of employees:



Top industries:

- Manufacturing
- Construction
- Miscellaneous Business Services
- Technology Services

34%

of respondent's companies received outside funding from private equity and venture capital market

Average company size:

50%

Less than $10 million in total revenue

50%

$10 million or more in total revenue

Spotlight on:

Directors & Officers

Tony Galban
Senior Vice President
D&O Product Manager

Chubb's most recent private company survey revealed that more than a quarter of participating companies experienced Directors & Officers (D&O) losses during the previous three years, though more than half had not purchased this line of insurance. And so the survey findings, combined with Chubb's long experience in this area, tell us there's a clear disconnect between executive assumptions about their companies' exposure and the potential risks that they actually face.

An important contributing factor to that disconnect may come from the fact that D&O insurance insures against wrongful acts by private company directors, officers and employees. Many private companies tend to believe that their behavior could not result in legal action.

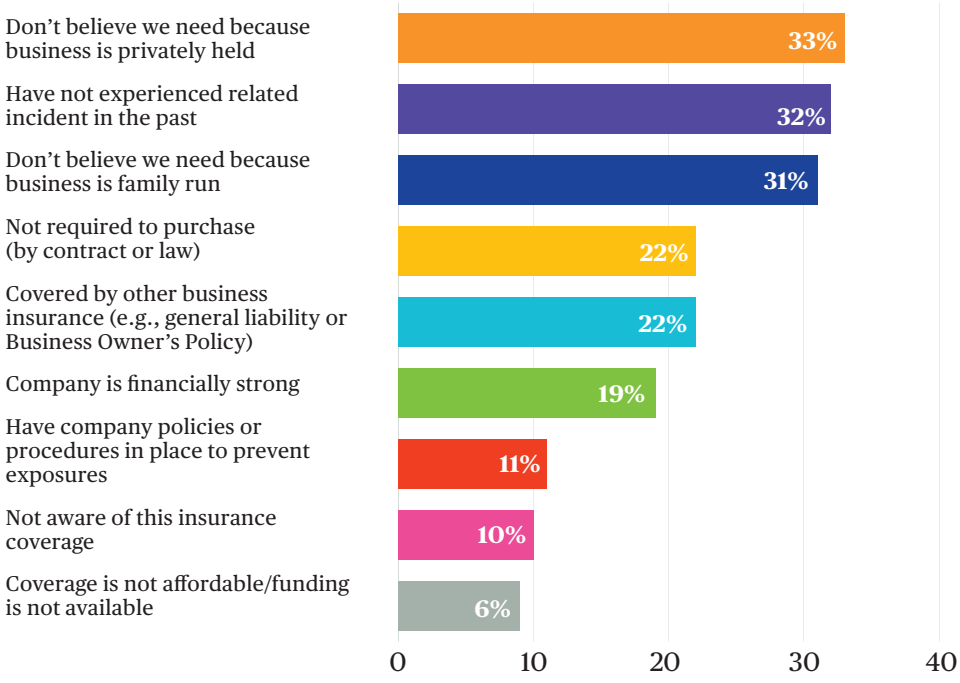
In this same vein, small or family-owned businesses often report that since "everybody loves us," they would never be subjected to a lawsuit.

Many companies also assume that their general liability insurance offers adequate coverage for any event that might result from their actions or behavior. Unfortunately, this is not the case. General liability insurance typically insures against losses involving bodily injury or property damage, but does not step in when there has been a failure to act by the company's directors and officers. When that happens, those who might sue can include anyone having an association with the company – customers, vendors or suppliers, government agencies, competitors, and partners or shareholders.

43% of responding companies indicate they currently purchase D&O insurance

Top Drivers of Non-Buyers

Of those who do not currently purchase D&O insurance, 1/3 feel they don't need it because they are either privately held or family run.



What a D&O Loss Looks Like – and its Impact

More than 1 in 4 (26%) private companies reported experiencing a D&O loss in the last three years

$399,394[1]

The average reported D&O loss

The most common losses are related to:

Customer sues the company and/or its directors or officers for any reason other than physical injury, product failure, or impairment

Vendor or supplier sues the company and/or its directors and officers

Competitor sues the company and/or its directors and officers

Government agency fines or sues the company and/or its directors and officers

Partner or other shareholder sues the company and/or its directors and officers

Director or officer is sued in connection with the purchase or sale of any equity or debt securities

How Private Companies Can Help Protect Themselves from a D&O Loss

- **Broaden the perspective:** When setting up crucial operational structures for a private company, outside experts of all kinds should be hired to assist.
- **Formalize operational structures:** Critical areas of operation should be formalized, such as accounting practices, areas requiring legal care or compliance, risk management practices, and employment practices, including hiring and vacation policies, bonus structures, and determining compensation levels. Also, a company code of ethics and mission statement should be created with the understanding that they could prove legally significant, since written documentation of all kinds can counter erroneous claims by providing published proof.
- **Diversify the Board membership:** To avoid a myopic orientation, especially when a company is poised to grow, board members who are experts in the field should be hired, rather than those with a company association who will inevitably limit, rather than diversify or broaden, the perspective.

Spotlight on:

Employment Practices Liability

Michael Schraer
Senior Vice President
EPL Product Manager

A key finding from Chubb's Private Company Survey was the fact that more than half the respondents listed attracting and retaining quality employees as their top employment challenge. That being the case, it behooves companies to pay special attention to the area of Employment Practices Liability (EPL), since fostering a respectful workplace – and addressing and resolving any situations that run counter to that cultural goal – will help them meet the challenge of attracting and keeping needed talent.

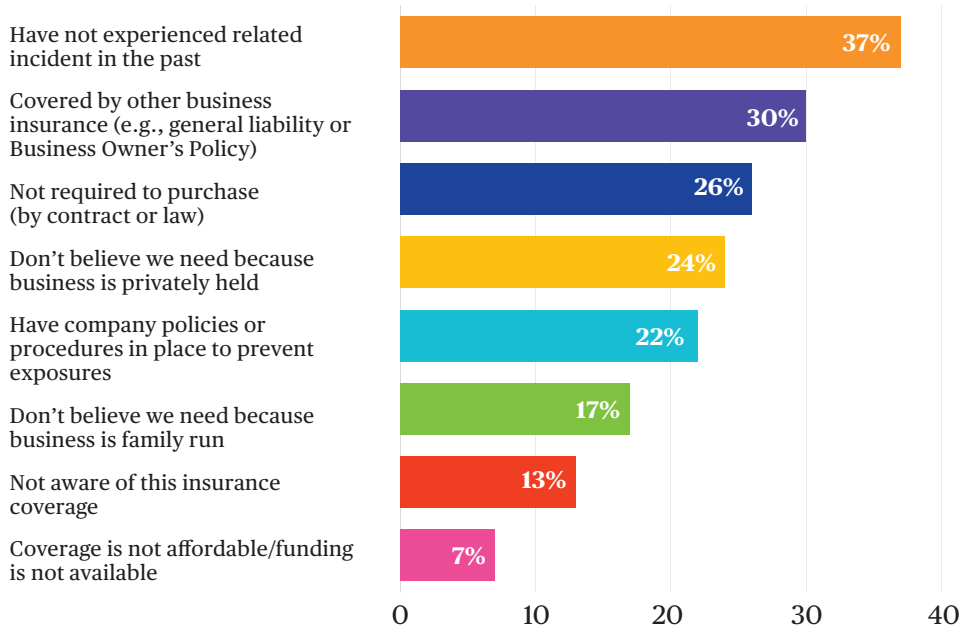
Apart from this finding, EPL claims relating to harassment, bullying, retaliation, and discrimination represent the majority of all management liability related actions. It is heartening to see that 65 percent of the respondent companies purchase EPL insurance. Among those non-buyers of EPL coverage, though, one third erroneously assumed that this area was already covered through other insurance policies. That could prove to be a costly misconception, especially when you consider everything a good EPL insurance policy can address.

So what should private companies look for from their EPL policies? Coverage should include access to a panel of pre-vetted and competitively priced top-notch employment defense firms, removing the need for a company to locate a trustworthy law firm quickly while in crisis mode. Good EPL coverage should also include a range of loss prevention and mitigation resources. These can include a toll-free hotline to access employment legal advice as well as online resources for training and education on employment matters of all kinds and template policies and procedures that can be useful in documenting, let's say, the anti-harassment steps a company has taken.

65% of responding companies indicate they currently purchase EPL insurance

Top Drivers of Non-Buyers

Of those who do not currently purchase EPL insurance, 1/3 feel they don't need it because they think it's covered by other business insurance.



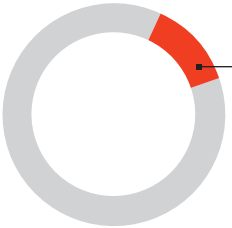
What an EPL Loss Looks Like – and its Impact

More than 1 in 4 (25%) private companies reported experiencing an EPL loss in the last three years

$102,915[2]

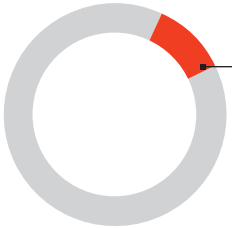
The average reported EPL loss

Sexual harassment is the top reported EPL issue:



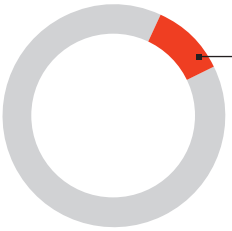
13%

An employee makes an allegation of sexual harassment in the workplace



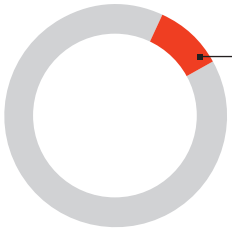
11%

An employee makes an allegation of workplace bullying



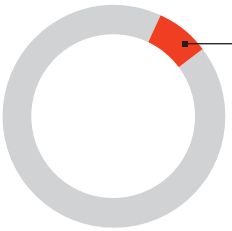
11%

An employee or former employee sues the company, its employees, the company's in-house counsel and/or its directors for employment related matters



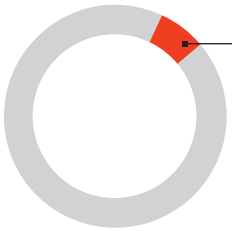
10%

An employee files a discrimination complaint with the Federal Equal Employment Opportunity Commission or any other state agency



8%

An employee makes an allegation of retaliation in the workplace



7%

An employee makes an allegation of misuse of social media for hiring/ firing purposes

How Private Companies Can Help Protect Themselves from an EPL Loss

- **Establish, maintain and consistently follow HR policies and procedures:** A legally vetted employee handbook stating the company's policies and procedures, including formal guidelines for mitigating EPL concerns, should be readily available and procedures should be followed consistently.
- **Train and certify employees:** Mandatory HR training should be required for harassment, discrimination and related workplace issues that could lead to lawsuits. Employees and executives should be required to read and sign off on the policies and procedures they must follow as a condition of employment.
- **Document all actions:** All employment practices-related actions taken should be documented in order to defend against possible future claims.

Spotlight on:

Cyber

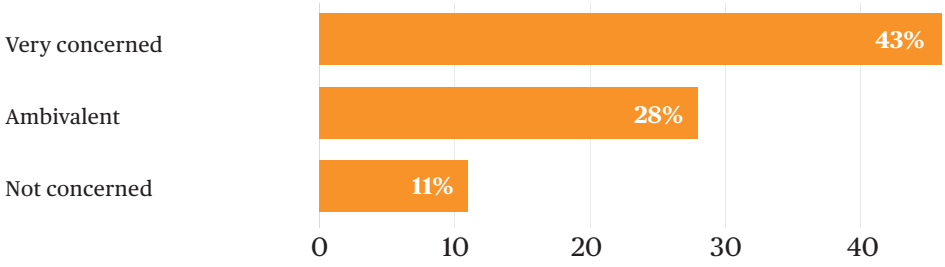
Matthew Prevost
Senior Vice President
Cyber Product Manager

One myth that is common among 85 percent of the executives at small and midsize private companies is that their organizations are not sufficiently large enough to interest cyber criminals. Unfortunately, the opposite is true. Cyber criminals are keenly aware of that widespread assumption, and 60 percent of all attacks are against small and midsize companies[3] for that very reason: cyber criminals know these organizations are less likely to have the resources in place to protect themselves with the robust cyber security measures employed by bigger enterprises.

Cyber criminals particularly like to target small and midsize healthcare organizations as many of these organizations are in the middle of – or just beginning – the inevitable migration to electronic medical records. In this scenario, criminals find

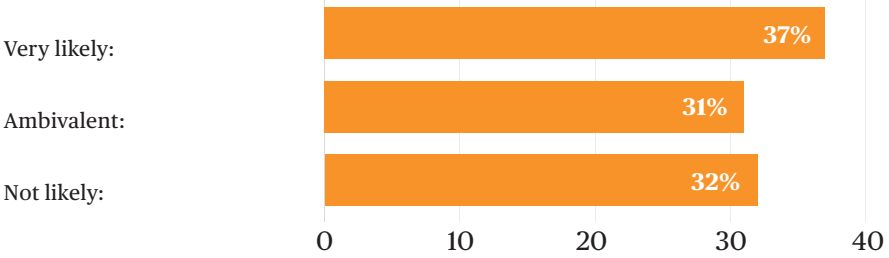
Who Is Buying Cyber Coverage?

Nearly half of those with access to third-party non-public data are very concerned about a potential third-party cyber breach in the next 12 months.



But only 39% of all responding companies currently purchase cyber liability insurance.

And only 1/3 of all responding companies plan to purchase cyber insurance in the next year:



52% of responding companies indicate they have access to third-party non-public records or data

(e.g., non-public customer or employee information such as telephone, address, government-issued ID numbers, medical or healthcare records, credit or debit card numbers, passwords, etc.)

it relatively simple to steal Protected Health Information (PHI), which is valuable on the black market.

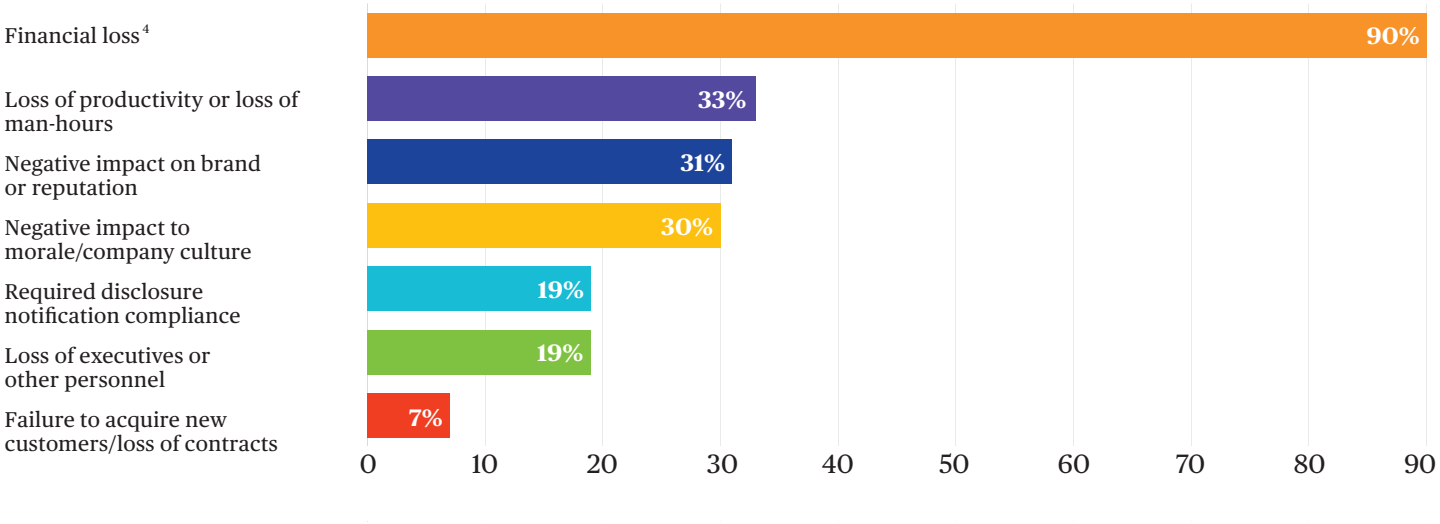
Another group favored by cyber criminals are small to midsize retailers struggling to transition to the EMV (Europay, Master Card, Visa) or chip and pin credit card payment acceptance. The changeover period makes retailers far more vulnerable to heightened cyber risk than those in other industries. Further, when credit cards are compromised by a hack where a retailer elected not to transition to EMV, that retailer may face additional liability related to the adjudication process for PCI-DSS, a set of security controls that all businesses are required to implement to protect credit card data.

An additional area where private companies sometimes run into trouble occurs when they outsource parts of their operation to outside vendors. Take for example a company that outsources its IT functions to a vendor. Despite the common misconception, the private company's exposure and responsibility for any future cyber attacks have not been transferred to the IT vendor, as the company is often still responsible for losses if their data is compromised.

Top reasons respondents haven't purchased cyber liability insurance:

What a Cyber Loss Looks Like – and its Impact

Financial loss is the top reported impact of a cyber incident:



How Private Companies Can Help Protect Themselves from a Cyber Loss

- **Make cyber security a top-down priority:** The development and implementation of cyber security measures like those identified below should require the involvement of C-Suite executives and all members of a private company's leadership team. Such measures should become an integral part of a company's culture.
- **Develop an incident response plan:** A robust and well-thought-out incident response plan should be created. Having the needed response service vendors already on board and ready to act is critical when a cyber incident occurs, including forensic firms, call centers, crisis management/public relations professionals, legal assistance, and more.
- **Educate employees:** All employees should be required to participate in continuous educational programs and training about cyber security policies. This type of training is critical for all employees and executives at all levels of the organization.
- **Update software:** Software should be updated regularly, and patches for known vulnerabilities downloaded as soon as they are available.
- **Vet the vendors:** Any outside vendors should be thoroughly vetted to ensure they are positioned to handle the ramifications of a large breach.
- **Implement strong password hygiene:** Require all employees to have strong password protection, which needs to be updated regularly. Also use dual factor authentication where available.
- **Purchase cyber insurance:** A good cyber policy is not just financial insurance in the event of an incident, even though such incidents can result in substantial losses. More importantly, a good cyber insurance policy integrates loss mitigation services to help prevent losses before they occur and incident response services to help limit exposure when an event occurs.

Spotlight on:

Commercial Crime

Christopher Arehart
Senior Vice President
Crime, Fidelity, and Kidnap/Ransom & Extortion Product Manager

56% of responding companies indicate they currently purchase commercial crime insurance

Private companies are increasingly exposed to substantial losses stemming from internal theft, as employees are inherently trusted with company property, inventory, money, and computer systems as part of running the business. Company assets are particularly vulnerable to white collar employee theft when there are few controls, or when the in-place controls aren't strong enough to guard against crimes of this nature.

A compounding factor with internally committed white collar crimes is that they may not be identified for months, years, or even decades. That's because an employee who knows how to circumvent whatever loss controls are in place can easily hide theft by altering relevant records, submitting false invoices, or budgeting for a nonexistent project.

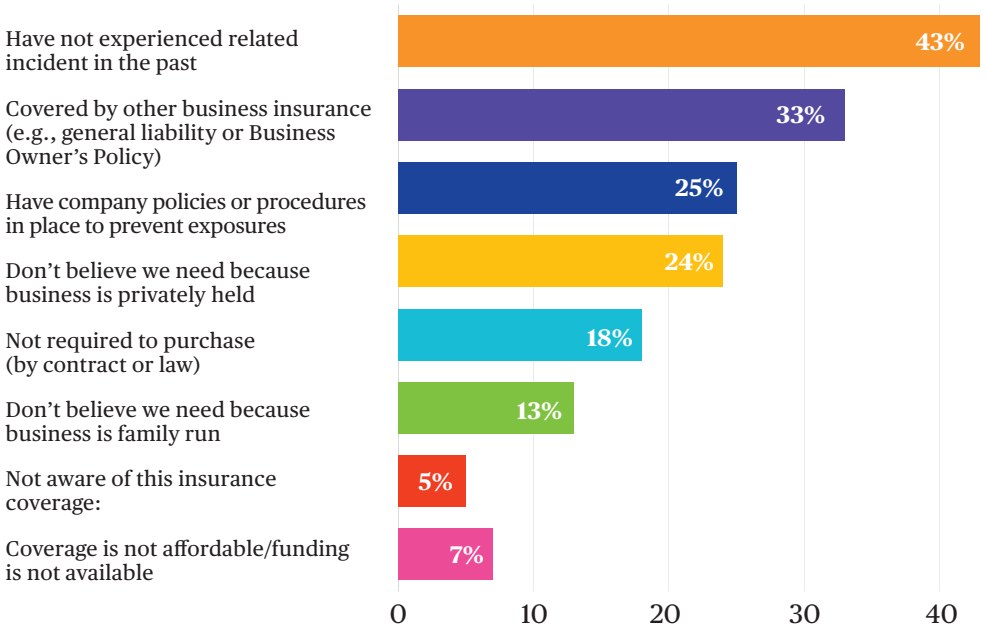
There are a handful of reasons why a previously honest employee may turn to theft. Among them are pressures in that employee's personal life, requiring large sums of money to support an addiction, wanting to "keep up with the Joneses," and even developing and harboring a grudge against the company. It surprises many, but the typical employee who turns to white collar crime is male, has been employed by the company for a decade or more, has a college degree, is in his forties, and has access to the financial assets of the company.[5] Due to being in a position of responsibility (working in the Accounting Department, for instance), this employee has the means to cover up his or her fraud, at least temporarily.

Even more nefarious is the rising risk of imposters who seek to trick employees into making payments based on fraudulent emails and invoices. With reported and actual losses measured in the billions of dollars, according to the FBI, such social engineering frauds are here to stay.

It's completely possible for white-collar employee fraud and related crimes to lead to substantial losses. With more than half of fraudsters working with others to collude, even the best control environment can be compromised.[5] As a result, private companies are well-advised to purchase insurance that specifically covers employee theft and other financial crimes committed by third parties, since most Property & Casualty insurance policies do not provide enough coverage to adequately reimburse the staggering amounts stolen by trusted employees or outside thieves.

Top Drivers of Non-Buyers

Of those who do not currently purchase commercial crime insurance, most feel they don't need it because they haven't experienced an incident in the past or they believe it's covered by other business insurance.



What a Commercial Crime Loss Looks Like – and its Impact

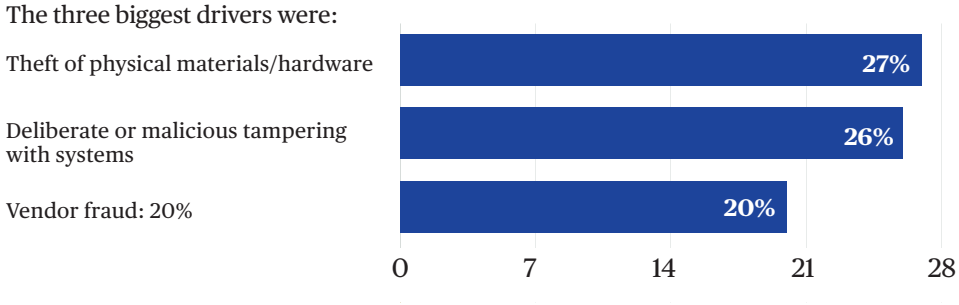
$297,009[6]

The average reported commercial crime loss

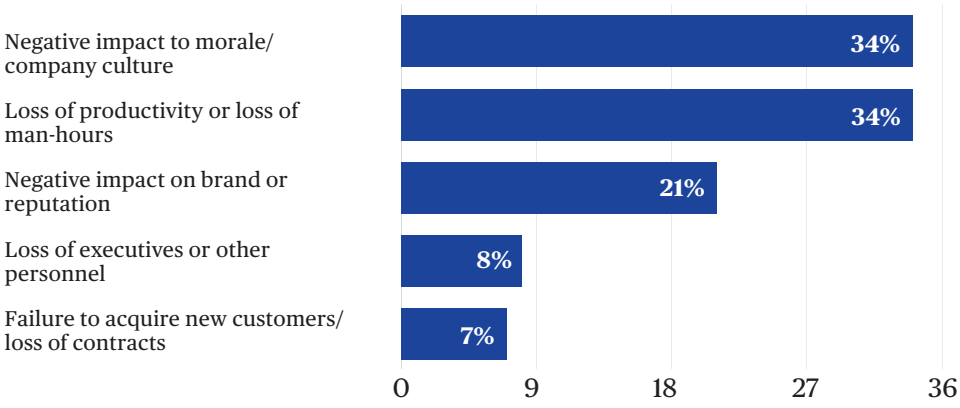
In the prior three years, 22% of companies reported having had an employee steal company funds, equipment, inventory or merchandise.

1 out of 25 companies report that a third party tricked an employee into transferring funds to a criminal through impersonation of an executive or business partner.

Of those companies that reported having experienced a loss event related to fraud, more than a quarter reported losses relating to a theft of physical materials/hardware. The three biggest drivers were:



Those same companies reported the following impacts as a result of their fraud-related loss:



Companies should keep in mind that embezzlement and fraud aren't necessarily committed against their own organization. They can also be against a client. 9% of respondents reported employees stealing funds, equipment, inventory or merchandise from a client.

How Private Companies Can Help Protect Themselves from Commercial Crime Losses

- **Establish a system of checks and balances:** Divide the responsibilities involved in ordering and paying for purchases, so the person who writes the checks is different than the person who signs the checks, and is different, once again, from the person who reconciles the bank statements. In this way, no one person has total control over the payment process, and the likelihood of theft is reduced.

- **Maintain a master list of vetted vendors:** Create a list of all vendors and suppliers who may be paid for purchases made by employees, being sure to verify their authenticity prior to adding or changing their information. Vendor Tax ID numbers can be verified with the IRS, and a simple online search can help confirm physical addresses. Periodically speak with vendors over the phone by calling known phone numbers, rather than relying solely on email to communicate.

- **Monitor open accounts:** Safeguard corporate bank accounts by regularly reviewing bank statements and monitoring transaction histories to help identify fraud from both employees and other criminals who may have obtained online access to the accounts.

- **Partner with the bank:** Take advantage of the fraud prevention services offered by the bank who handles the company accounts. To prevent check fraud, for instance, banks can be given a list of all checks legitimately written each month; if additional checks are presented, they'll be investigated for theft. If wire transfers are not regularly performed to banks outside of the U.S., request the bank to automatically block them.

- **Implement additional verification processes:** Request verbal verification for the wire transfer of all funds over a certain amount, in addition to the two-factor authentication process that many banks use.

- **Open a hotline:** Install an employee hotline for reporting internal fraud as an anonymous tip. According to the Association of Certified Fraud Examiners, the use of a hotline has proven effective in reducing the severity of fraud, as well as the amount of time that an internal crime was allowed to continue undetected. In 2016, nearly 40 percent of crimes were reported by tip, whereas only 16 percent were found by internal audit.[7]

About Chubb's Private Company Management Liability Practice

Privately held companies, regardless of size, are threatened by multiple liability and criminal exposures. While no private company is immune to these exposures, organizations can help mitigate those risks with the right insurance accompanied by comprehensive risk management resources and services. Chubb's suite of management liability products is designed to help protect private companies, offering tailored insurance coverage backed by superior claim service and financial stability.

A few facts about Chubb:

- Chubb is the world's largest publicly traded P&C insurance company, and the largest commercial insurer in the U.S.
- Chubb operates in 54 countries, with approximately 31,000 employees serving a diverse group of clients worldwide.
- As of December 2017, Chubb has total assets of $167 billion, and total capital, which reflects our capacity to take on risk, of $64 billion.
- Chubb's core operating insurance companies maintain financial strength ratings of AA from Standard & Poor's and A++ from A.M. Best.

About This Report

Chubb is pleased to provide this snapshot – our sixth since 2003 – of how private companies in the U.S. are contemplating and managing a number of important exposures.

In 2016, Chubb commissioned Chadwick Martin Bailey, a leading provider of data-driven market strategy solutions, to survey 600 decision makers in U.S. private companies to ascertain concern about corporate risks and uncover risk mitigation strategies and to identify the prevalence of insurance ownership.

This report features selected findings from Chubb's 2016 Private Company Risk Survey, as well as up-to-date information gleaned from reliable third-party sources to help add depth to our analysis. We hope you find the information to be interesting and useful as you navigate your company through today's challenging business environment.

[1] Total financial loss percent represents those with losses greater than $0.

[2] Total financial loss percent represents those with losses greater than $0.

[3] Millaire, Pascal; Sathe, Anita; Thielen, Patrick. (2017) What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets. (https://www2.chubb.com/us-en/_assets/doc/17010201-cyber-for-small_midsize-businesses-10.17.pdf)

[4] Total financial loss represents those with losses greater than $0.

[5] KPMG. (2016) Global Profiles of the Fraudster: Technology Enables and Weak Controls Fuel the Fraud. (https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profile-of-a-fraudster-infographic.pdf)

[6] Total financial loss represents those with losses greater than $0.

[7] Association of Certified Fraud Examiners (ACFE). (2016) Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study. (https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf)

Contact

For more information about Chubb's solutions for private companies, contact:

Leigh Anne Sherman
Executive Vice President
lsherman@chubb.com
860.408.2615

www.chubb.com/us/managementliability

Chubb. Insured.℠