2020 Cyber Security Risk Report

Solving the Cyber Puzzle:

The Unexpected Ways Cyber Risk Impacts Your Business

Published: February 2020

AON

Empower Results®

Table of Contents

20 years of Cyber Solutions in 2020

Message from the CEO

This year, Aon will celebrate 20 years of delivering Cyber Solutions to clients. In 2000, the newly formed Aon Technology and Telecommunications Group issued the first insurance policy that covered cyber exposures as part of an Errors and Omissions placement. That same year, Stroz Friedberg was founded. Today, we are united as Aon's Cyber Solutions and our greatest advantage is the ability to leverage our experience to benefit the needs of our clients. From Risk Transfer, Quantification, Cyber Risk Consulting, Incident Response, Digital Forensics, Investigations and Intelligence, and eDiscovery—we have worked and solved some of the world's most difficult challenges.

Our experience and proven ability to exceed clients' expectations continue to set us apart in an increasingly crowded field of competitors. There are no other firms that bring our holistic suite of solutions to market and can demonstrate the continuity of performance across these disciplines like we can at Aon's Cyber Solutions. Many firms can only promise the potential to do what we have already done.

As we reflect upon this significant milestone, it is the perfect time to share our 2020 Cyber Security Risk Report: ***Solving the Cyber Puzzle: The Unexpected Ways Cyber Risk Impacts Your Business***. This year's Report demonstrates the breadth and depth of our collective understanding of cyber risk across Aon. In it, we focus on the unexpected ways that cyber risk impacts clients, in six less-appreciated areas: Intellectual Property, Mergers and Acquisitions, Retirement, Executives, Computer Crime and The Corporation. Our experience allows us to see the entire puzzle and how the pieces fit together. As such, part of the Report provides a playbook for each highlighted risk to help organizations "solve" the ever-more-complex puzzle that is cyber risk.

As outlined in our recent white paper, ***The Cyber Loop: Managing Cyber Risk Requires a Circular Strategy***, there is nothing linear about cyber security. Solving the cyber puzzle requires a tactical mix of technology, people and process in the form of assessment, quantification, insurance and incident response readiness. Regardless of where your organization is in its digital journey, the Cyber Loop can help insulate your company from a variety of cyber risks. And importantly, it acknowledges that cyber risk is an enterprise risk, not solely a technology concern. Companies have a duty to understand that corporate risk–and the threat to business continuity and customer data–is at stake.

Every business has a cyber story. We look forward to continuing the story with you for another 20 years as your chosen cyber security partner. We remain committed to helping organizations uncover and quantify cyber risks, protect critical assets and recover from cyber incidents.

Jason Hogg
CEO
Aon's Cyber Solutions

Intellectual Property
THE PUZZLE

Theft, misappropriation or infringement of intellectual property (IP)—assets that lack physical substance such as patents, trademarks, copyrights, data rights and trade secrets—poses a significant and growing risk to your organization.

From 2005 to 2018, the value of intangible assets held by the five largest companies by market cap increased from $9.28 trillion to $25.03 trillion.[1] IP is core to innovation and business growth, and with cyber incidents targeting IP on the rise, the danger shows no sign of stopping.

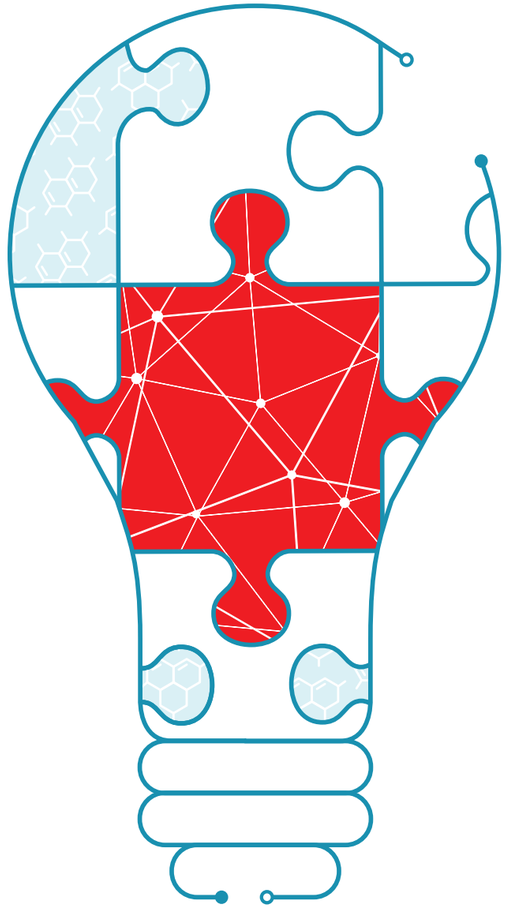
In its 2017 Update to the Report on the Theft of Intellectual Property, the IP Commission organizes the cost of American IP theft into three categories—counterfeit or pirated tangible goods, software piracy and trade secret theft—and estimates the annual cost to be more than $225 billion, and possibly as high as $600 billion. Baker McKenzie suggests this to be a $1 trillion a year problem. The threat comes from several different actors, including current and former employees, the organization's supply chain, third-party vendors and state-sponsored cyber criminals or hackers.[2] Intellectual property losses are often complex; IP is often more difficult to value and insure when compared to traditional property losses, for example. Costs associated with IP litigation, damages and theft can be devastating. Despite the importance of IP to an organization, and the percentage contribution of IP to the total assets on the balance sheet, physical assets, in the form of property, plant and equipment, have much more coverage by insurance (60% versus 16%).[3]

A key concern is the theft of trade secrets, which according to the U.S. Chamber of Commerce is valued in excess of $5 trillion. Trade secrets are defined differently around the world, but broadly, according to the World Intellectual Property Organization (WIPO),[4] trade secrets include "any confidential business information that provides an enterprise a competitive edge." In December 2019, the federal government brought criminal charges against two former technology company employees accused of stealing trade secrets. In its request to monitor the location of the suspected perpetrators, the prosecution expressed "deep concerns" that the former employees would try to flee the U.S. One worked on a secretive self-driving car program and allegedly took files related to the project before disclosing his intent to work for a foreign competitor. The second purportedly took more than 2,000 files containing "manuals, schematics, diagrams and photographs of computer screens showing pages in secure databases," with intent to share.[5]

Another notable case is the theft and subsequent copying of an Australian metal detector company's product designs when a hacker broke into an employee's laptop via a hotel WIFI connection during a business trip to China. The company was forced to slash prices to compete with counterfeits and spent considerable sums on private investigators. As a result, its net profit fell to A$9.2 million ($9.76 million[i]) from A$45 million ($43.9 million[ii]) just a year earlier.[6]

With this backdrop, it makes sense that nearly half of 400 senior executives report that trade secrets are more important than patents and trademarks. However, less than one-third of companies have taken basic measures to protect trade secrets,[7] even when it is estimated that the value of trade secret theft represents one to three percent of U.S. gross domestic product (GDP).[8] Now in 2020, the significance and protection of IP need to be placed at the core.

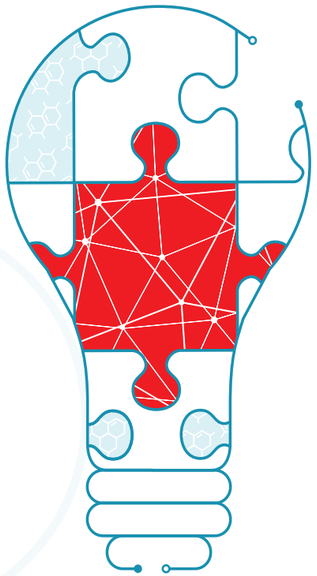
i. June 30, 2014 Exchange rate: 1 – 1.0604, www.exchangerate.org
ii. June 30, 2013 Exchange rate: 1 – 1.0956, www.exchangerate.org



IP theft is estimated to be a **$1 trillion** a year problem.

Less than 1/3 of companies protect trade secrets.

Intellectual Property
THE PLAYBOOK



Although Intellectual Property strategy, valuation and protection are issues for a board of directors to consider, IP protection resides in and across the remit of many corporate stakeholders including innovation officers, CTOs, heads of IP and human resources.[9]

Organizations should allocate appropriate resources to the strategy, valuation and protection of IP based on a cost-benefit analysis.

An important step in solving the IP puzzle is for organizations to **identify critical assets**, sometimes referred to as "crown jewels," to understand what Intellectual Property the company holds and where it sits across the organization's operating environment. Is the data stored on a network server, in cloud storage, on an employee's personal device or a third-party vendor system? What, exactly, is the essence of the Intellectual Property? Once identified, assets can be tagged, classified and protected–both physically and digitally. The use of advanced control technologies and processes should be contemplated, including encryption, access controls, monitoring and logging technologies. These controls should be augmented by a robust **employee training** program. People are often the weakest link in an organization and IP is vulnerable to human error or carelessness. Training that addresses how IP can be unintentionally exposed is vital.

Quantifying the value of IP is an important step on the way to evaluating risk appetite and then insuring the value of the IP that could be compromised. Harvard Business Review reports that intangible assets make up 80% of the value of S&P 500 companies. Financial analytics and modeling can help inform risk transfer methods, such as limits and scope of **intellectual property insurance** coverage. As IP theft becomes a more considerable issue and competitors look to increase market share in any way, companies may also need to defend themselves against accusations of IP infringement or theft. As a result, businesses may be exposed to potentially significant financial losses and reputational damage.

Even with adequate and appropriate training, IP can still be vulnerable. The intelligence gathered during a strategic assessment can inform and strengthen an organization's **incident response**. In the event of a breach, knowing where the IP is held within the network helps the response team to more rapidly identify what data might have been impacted or exfiltrated. Was IP data compromised? And importantly, what exactly was in that data? If it can be determined that IP was misappropriated, organizations can more rapidly set a defensible path to try to mitigate the impact of the IP theft and preserve the secrecy of their most valuable assets by bringing quick injunctions against the third parties. The effective management of incident response, including forensics, is critical as it may serve to support subsequent litigation or loss recovery.

What, exactly, is the essence of the organization's **intellectual property?**

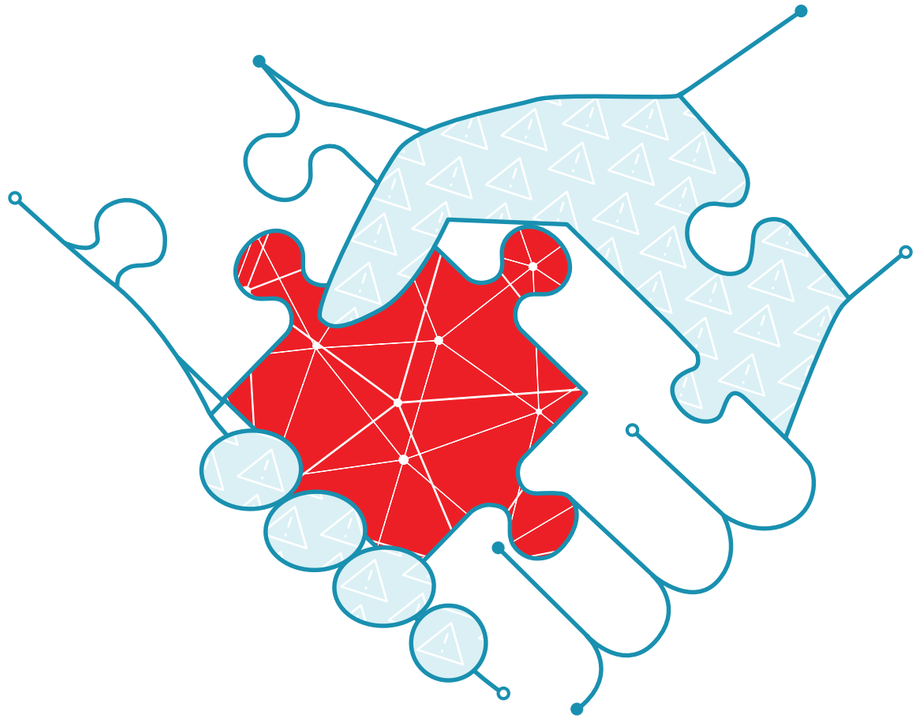
Mergers and Acquisitions
THE PUZZLE

The years 2014–2017 witnessed a 96% rise in mergers and acquisitions (M&A) globally,[10] and over the past two years close to 50,000 M&A transactions were announced worldwide, worth a total of more than $3.5 trillion a year.

When merging with or acquiring another company, an organization may unintentionally inherit the target company's cyber risks and vulnerabilities. Executing deals without understanding the cyber posture of the target company jeopardizes investment capital and future returns can bring legal or operational ramifications, and even threaten brand reputation and value.

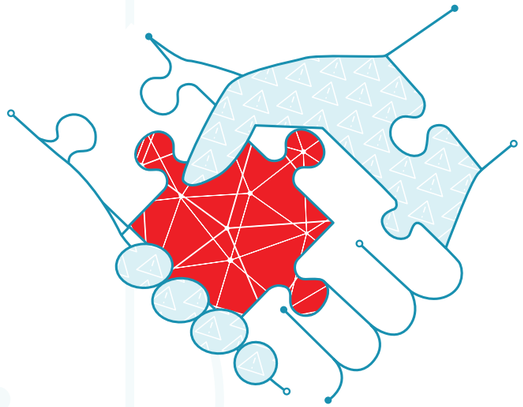
Cyber threats in M&A are serious and can be fatal for businesses: compromised networks, customer data or IP actively being sold on the dark web, historic data breaches or regulatory noncompliance all pose a material risk to investor capital. Yet, less than 10% of deals globally include specialist cyber security due diligence as a part of the deal process,[11] often concluding that cyber security is best examined post-deal. The M&A puzzle is complicated. Would the deal strategy change, for example, if investors knew that the target's customer information is being sold on the dark web? Or that the flagship software application requires a significant cyber investment? What vulnerabilities might the target's network introduce that need to be factored in prior to deal close or on day one?

Recent examples illustrate the severity of the risk. One significant case comes from the hospitality industry, a sector that has witnessed an increase in consolidation over the past few years.[12] In a major breach, the information of up to 500 million guest records was compromised, triggering potential consequences including data regulatory fines and reputational damage. Notably the compromise occurred within the network of a company that had been acquired for $13.6 billion two years before the incident was detected. Reportedly, the hacker(s) had access to the acquired company's network for approximately two years before the acquisition, and four years before the breach was detected. A regulator cited an apparent lack of pre-deal cyber security due diligence as being justification for a proposed $123 million fine under the European Union's General Data Protection Regulation (GDPR). In another case, the breach of a technology firm resulted in the final purchase price being reduced by $350 million.[13] This was in response to disclosures made post-deal writing and the acquiring company was obliged to share liabilities regarding the breach investigation and pay a $35 million penalty to settle charges that it "misled" investors.



Less than **10%** of M&A deals globally include specialist cyber security due diligence.

Mergers and Acquisitions
THE PLAYBOOK



Leave nothing to chance when pursuing a merger, acquisition or divestment.

It is crucial to consider cyber risk before capital is released and the acquiring organization needs to evaluate the overall cyber security posture of the target. This security assessment needs to go beyond data breach risk to also examine the risks covered in this report, such as IP theft. Only then can the acquiring organization build an informed view of risks and costs from the outset and manage that risk across the transaction lifecycle.

Pre-deal, structured due diligence via a cyber **red flag review** is nonintrusive and revealing. This appraisal investigates the acquisition target and may include a scan of active and historic risks, a look at vulnerabilities including a dark web search and quantification of financial loss exposures. Using other tools, organizations can perform forensic analysis of the cyber risk accompanying a deal. In parallel, the acquiring organization is advised to execute a second-tier review or an **operational and technical review** that asks: Does the target have governance and policy in place to manage cyber security risks? Has the target taken reasonable steps to comply with data privacy regulations? This second-tier review delivers a fuller picture and can provide specific guidance on how to "de-risk" the deal and enhance valuation. The final, or third-tier review, requires permission to access the target's network and systems. Technical specialists can conduct ethical hacking exercises, review high-risk assets for evidence of historical compromise, evaluate critical technology vulnerabilities, assess source code quality and/or maintainability and determine legality of intellectual property (IP) ownership. This final tier builds a deep view of **cyber technical risk and source code issues** in advance of an acquisition, commonly during exclusivity.

Armed with knowledge, organizations can make strategic decisions on whether to execute the deal, negotiate specific terms to mitigate identified risk, negotiate on value or leverage insurance to offset the risk to investor capital. With risk transfer, **M&A insurance** has changed the way deal professionals allocate risk, using insurance to bridge the gap of one of the most fundamental issues in any M&A transaction: the potential post-closing erosion of value, either of the consideration received by the seller or the business acquired by the buyer.[14] Appropriate use of M&A insurance (also known as Representations and Warranties insurance or Warranty and Indemnity insurance) is gaining popularity. In 2018, over 45% of the addressable North American M&A market (private deals with enterprise values between $25 million and $10 billion) used M&A insurance, up from 34% in 2017.[15] In Asia, uptake in 2018 increased 40% year-over-year; and in Australia and New Zealand, there was 37% year-over-year growth in the number of 2018 deals using M&A insurance.[16] However, companies should be mindful. While such policies may cover cyber risk, it is limited to the representations in the purchase agreement on data, storage or cyber security controls, and ought not be placed in lieu of a **cyber insurance** policy. Acquiring companies should confirm if the target being acquired has a cyber insurance policy and the scope of cyber insurance coverage relevant to the transaction and the amount of potential financial losses.

Post-close, the acquiring organization should be prepared to launch a plan of action to address and remediate any known security weaknesses in the newly acquired organization's environment and should ensure that these risks are sufficiently addressed prior to establishing network connectivity or other integration activity. Additionally, any longer-term cyber risk remediation activities should be monitored to include periodic testing and assessment.

Use of M&A insurance in North America is up **11%** from 2017–2018.

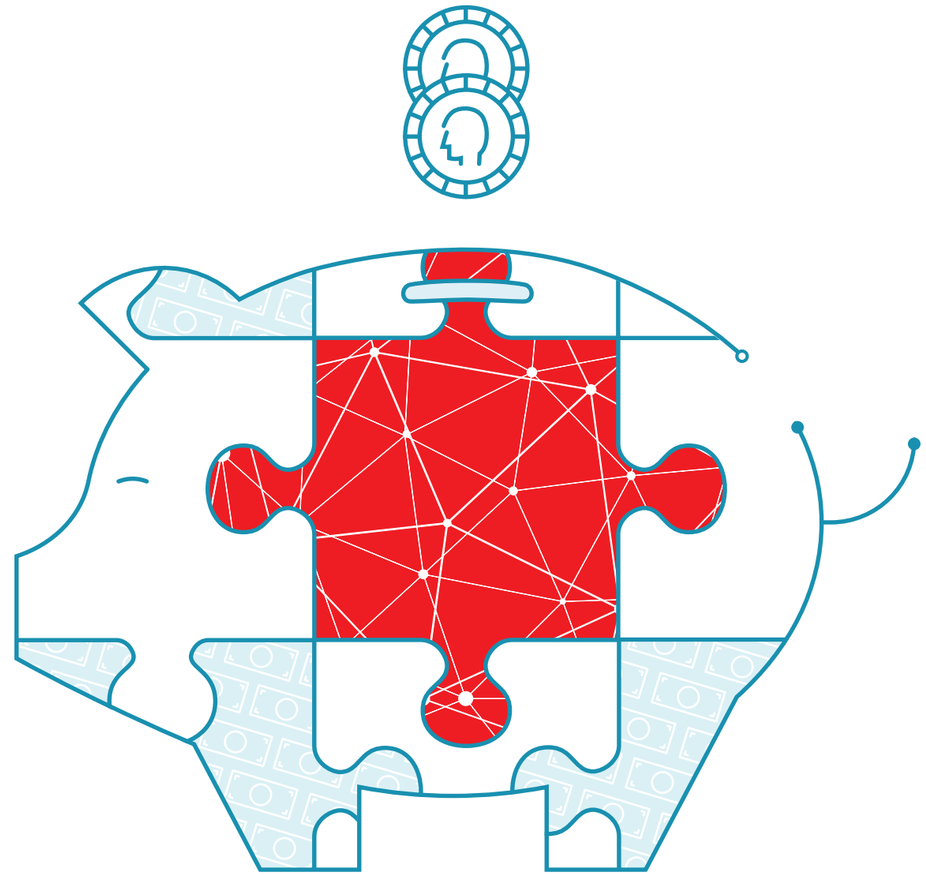
Retirement
THE PUZZLE

Retirement plans hold a wealth of personal and sensitive data and are a gateway to vast sums of money.

These plans are increasingly accessed from online platforms and mobile devices and thus are susceptible to breach. While many retirement plan hacks do not make headlines, reports in the media are becoming more prevalent. News of one breach broke when a U.S. municipality retirement plan, which boasted approximately $3.6 billion in assets, reported that $2.6 million was taken in the form of unapproved loans from 58 participant accounts.[17] Participants' personal information was used to set up web profiles that allowed loans to be taken. The company returned the funds to the accounts within five days, demonstrating the responsibility corporate plan sponsors are taking to make plan participants whole in the wake of theft.

To decipher the retirement risk puzzle, organizations must inquire: What is the fiduciary responsibility of the plan provider? The plan sponsor? Who owns the data? What privacy laws and regulatory reporting laws govern retirement plans and cyber security? Organizations commonly hold false confidence in the security of retirement plan data, thinking that all data sits within the four walls of the company as the plan provider. However, it is often a third-party record keeper holding plan data, potentially introducing additional risk for which the C-suite can be held accountable. In one case of a third-party record keeper, the CEO came under scrutiny for being slow to report after three data security incidents affected a U.S. municipality employee retirement association, a pension fund client with $56 billion of assets under management.[18] In the UK, almost a quarter of trustees of UK pension schemes have had no training on the risk of cybercrime.[19] Two-thirds of schemes currently have no documentation of cyber risks, mitigations and security policies and procedures.

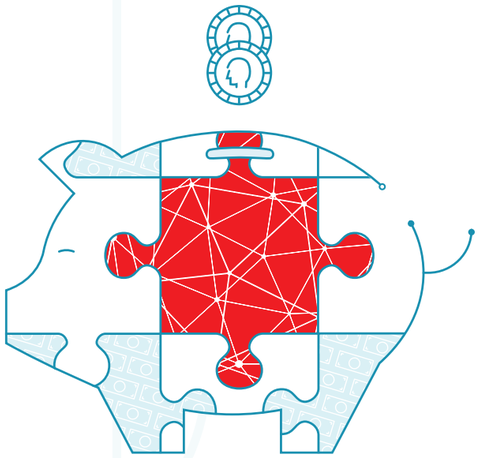
While not explicitly providing data security requirements, the U.S. Employee Retirement Income Security Act of 1974 (ERISA) imposes duties on fiduciaries, such as plan administrators, to administer plans prudently and for the exclusive benefit of participants. As we enter the new decade, cyber security is centrally located on the ERISA radar. Its Advisory Council on Employee Welfare and Pension Benefit Plans issued a report on "Cybersecurity Considerations for Benefit Plans," which asked the U.S. Department of Labor (DOL) to require sponsors to be familiar with the various security frameworks to protect retirement plan data.[20] Still pending in the U.S. courts is a case against a cosmetics firm that directly contemplates this fiduciary responsibility. A former employee is suing the company and a third-party benefits firm alleging they breached their fiduciary duty to secure her 401k retirement account after a six-digit distribution was executed from her account without her knowledge.[21]



Almost 1/4 of trustees of UK pension schemes have no training in cybercrime risk.

Organizations commonly hold **false confidence** in the security of retirement data.

Retirement
THE PLAYBOOK



Given the amount of data and money at stake, it is imperative that organizations see the whole cyber security picture when it comes to retirement plans.

Risk, technology and human resources teams are all crucial players, tasked with collaborating with plan providers to exercise due diligence and ensure security safeguards are in place.

An important first step in the retirement protection playbook is to conduct a **gap assessment** to examine vulnerabilities, along with the administrative, physical and technical protections enveloping the plan such as security governance, business operations security and relevant controls. The end goal is to protect data from unauthorized access and to ensure available technology, process and controls are utilized to safeguard plan data and funds. Accomplishing this is more complex than it might appear, as plan data resides in many forms. Security domains–both internal and external–need to be reviewed and third parties that have access to plan data and funds evaluated for their cyber security controls. Once security gaps and vulnerabilities are identified, a **risk mitigation plan** can be strategized and implemented then an **incident response** (IR) plan developed and put into practice. Within the IR plan, privacy regulations need to be thought through, ensuring the organization adheres to appropriate notification requirements.

Finally, evaluation of **risk responsibility** and **risk transfer** options is essential. ERISA requires that claims by plan participants be asserted against the plan fiduciary, making it prudent to have contractual specifications about data and asset security and methods to shift the loss to the service provider where warranted. Terms should be negotiated and periodically re-visited. Otherwise, differences may arise over which party is responsible for cyber security.[22] Depending on the type of loss, cyber insurance, fiduciary liability insurance or crime insurance may be available to transfer additional risk and indemnify the company.

The end goal is to **protect data** from unauthorized access.

Executives
THE PUZZLE

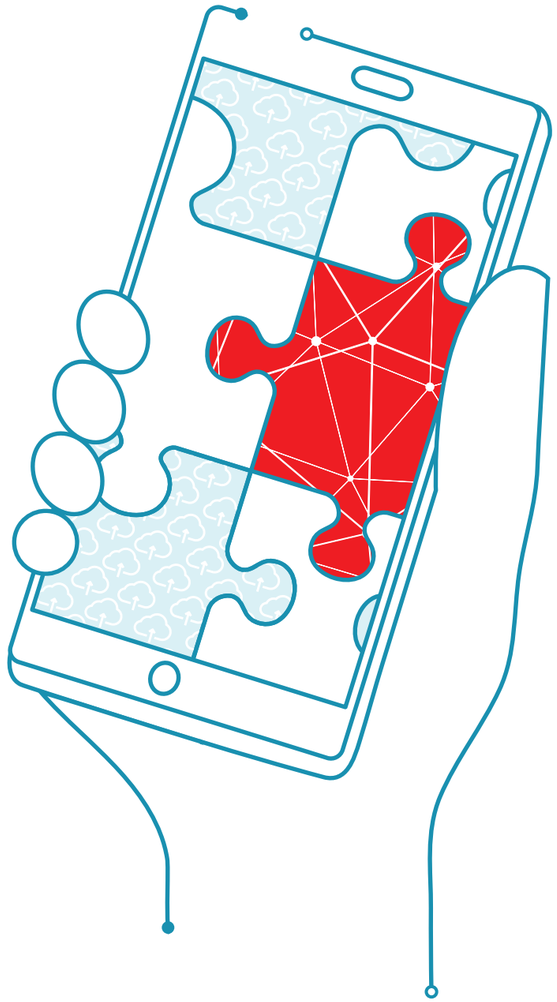
For attackers seeking a substantial payday, the C-suite is frequently the bullseye on the target.

C-level executives are 12x more likely to be pursued and 9x more likely to be victimized.[23] Executives are often the targets of social engineering techniques and compromise of web-based email accounts using stolen credentials is on the rise, with 60% of attacks involving hacking of a web application.[24] These leaders are pursued for many reasons: influence, reputational value and access to data of interest. However, it is financial reward that is the key motivation behind an executive breach. In 71% of executive breaches, financial motivation is in play,[25] with attackers seeking to benefit from ransomware or access to critical systems that hold the organization's data, such as employee and company data or intellectual property that can be used for advantage or sold for a price.

In an identity theft case, one Swedish security company CEO found himself victim when a fake loan application was approved in his name and a bankruptcy application subsequently submitted. The Stockholm District Court accepted the application and the CEO was declared bankrupt. The company's rapid response resulted in the removal of the bankruptcy within days, yet even in that short time the CEO was de-registered as chairman and member of multiple boards, requiring the need for reinstatement.

Executive personal financial accounts are also regularly targeted; 77% of high-net-worth individuals rank cyber risk as their number one concern and 75% of wealth advisors have been the target of cyberattacks.[26] Hackers are also motivated by the gain of strategic advantage and espionage makes up one quarter of C-level breaches.[27]

There are many underlying reasons for mounting executive risk. An increasing volume of cyber threats target executives due to their prominence in the media. Additionally, insufficient awareness and training programs related to cybercrime and frequent travel may increase risks for executives. It's not that the C-suite doesn't understand the gravity of cyber risk; 98% of these executives see cyber security as a key business driver, and many have some management responsibility for security.[28] It's the sophistication of the opponent, and the sheer rise in attack attempts that makes C-level executives more vulnerable, and makes solving this puzzle so complicated.



C-level executives are **12x** more likely to be pursued.

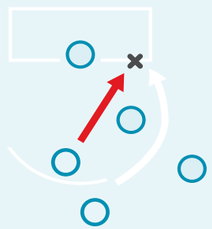
Executives
THE PLAYBOOK

Executive **vulnerability assessment** is a necessity and must consider not only areas of potential corporate compromise, but also personal and family member compromise.

Organizations need to begin securing the executive team outside of its physical and digital walls. The personal vulnerability of key executives is an increasing target of opportunity for threat actors. Once compromised personally, the executive may be leveraged or extorted to act on behalf of the attacker or even unknowingly carry the cyber threat into the organization.

The open and dark web are prime resources to evaluate an executive's security risk posture. Once the risk is gauged, mitigation steps can be taken. Such **mitigation actions** can include hardening of security weaknesses, a focus on information governance and data protection, training on phishing and social engineering techniques, direction on how to lessen open source exposure, as well as knowledge-sharing of emerging fraud schemes. Incorporation of security technology is also valuable for executives and their family members, such as identity theft monitoring, use of secure VPNs and password manager tools. However, as with any form of technology solution, it is only useful if implemented.

Insurance is also available to help executives mitigate the impact of identity theft, business email compromise (BEC) losses and ransomware attacks. While cyber insurance is available to protect the corporation against liability and financial loss arising out of a breach of corporate networks, executives may want to add a layer of personal cyber insurance protection outside the corporate veil. This coverage is available at many corporations as an executive or employee benefit. Personal cyber security insurance coverage continues to be an evolving area that companies should contemplate for their board, executives and employees.



Organizations need to **secure the executive team** outside of physical and digital walls.

Computer Crime
THE PUZZLE

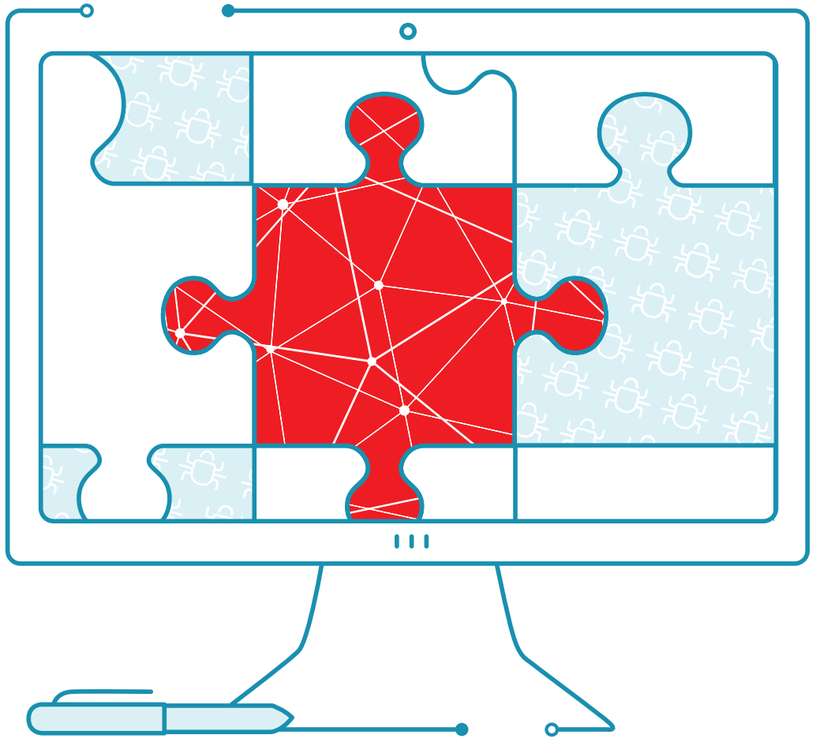
Cybercrime is on the rise globally. Statistics gathered by the FBI's Internet Crime Complaint Center (IC3) for 2018 show Internet-enabled theft, fraud and exploitation remain pervasive and were responsible for $2.7 billion in financial losses in 2018.

In the U.S., victims in the state of California lost more than $450 million through cybercrime.[29] For the small business, the risk is just as great with losses totaling almost twice as much per scheme as their larger counterparts.[30]

The median duration of a fraud scheme is 16 months. The longer a fraud lasts, the greater the financial loss. Business Email Compromise (BEC) and Email Account Compromise (EAC), embezzlement, financial statement fraud and allegations of bribery and corruption: the misconduct of just one individual can cause vast reputational and monetary damage. The 2016 Bangladesh Bank cyber heist pulled $81 million from accounts in just hours, not by stealing logins but by sabotaging the international money transfer system used to move currency.

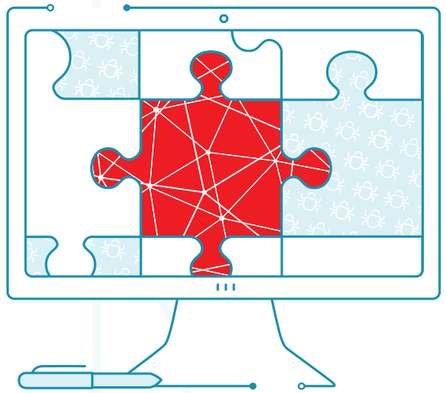
BEC and EAC crime are growing at an alarming rate. BEC targets businesses that often work with suppliers or vendors, while the EAC variation targets individuals who regularly perform wire transfer payments. BEC/EAC is estimated to target 6,000 victims monthly and has reportedly caused more than $12 billion in international and U.S. losses in less than five years.[31] Individuals and businesses alike are at risk for falling victim, with scammers becoming more sophisticated in social engineering techniques, often posing as fake CEOs or vendors. In 2019, one bank successfully halted a crime when its wire transfer authentication protocols circumvented a criminal's attempt to steal funds by posing as a business client CEO and submitting a wire transfer request via email. The business client's IT department determined that both the CEO and bookkeeper's corporate email accounts were compromised months earlier, and between then and the fraud attempt, the criminal monitored the email accounts and obtained the business' account number information as well as a sample of the CEO's signature.[32] Today, BEC may not always request a transfer of funds. Hackers are evolving and now seek to compromise legitimate business email accounts and personally identifiable information (PII) or tax forms (such as the U.S. W-2 form), for employees.

Within the computer crime puzzle, ransomware is a form of extortion not to be overlooked. Such attacks saw a 350% increase in 2018, with global ransomware damage costs predicted to hit $20 billion in 2021, up from $11.5 billion in 2019.[33] This past year bore witness to ransomware impacting companies large and small, public and private. Several U.S. cities fell victim, including large metropolitan areas like New Orleans and Baltimore. A more recent twist is not only encryption of the network for a ransom, but if the victim refuses to pay, then the attackers release sensitive company data on the internet–turning a ransomware-based business disruption into a data breach. Several prominent ransomware groups started publishing data stolen from victims who refuse to pay. One has created a public website identifying recent victim companies that have chosen to rebuild their operations instead of quietly acquiescing to their tormentors.[34]



Global ransomware damage is expected to hit **$20bn** in 2021.

Computer Crime
THE PLAYBOOK



To guard against cybercrime, a proactive cyber security and **fraud risk assessment**, combined with a **gap analysis**, can help identify vulnerabilities and provide a path to pinpointing your organization's risk.

Next, instituting the right **controls** to guide customer and vendor relationships will aid in reducing fraud and cybercrime exposure. The following questions must be painstakingly explored: Does the organization have a procedure in place to verify new customers prior to initiating any financial transaction? How are fund transfer instructions accepted, for example: telephone, fax, email, text or other similar method? For vendors, how does the organization confirm requested changes to contracts or banking details? Are change confirmations sent, and if so, to whom and via what method? Controls across voice and electronic initiated fund transfers also need to be evaluated even as they span business units and regions.

Not to be overlooked is **continuous cyber education**. This curriculum should be customized for employee categories, considering various characteristics such as seniority and data access rights, travel habits and overall cyber risk profile. It is recommended that training extend from simple concepts—such as the importance of strong passwords—to content covering common and current scams and how to avoid being a victim. Deeper concepts, such as verifying identities and the legitimacy of online communication, are also critical to explore.

Even with controls and training in place, the risk is pervasive. **Risk transfer via insurance** is available, yet it can be a challenge to know which coverage is intended to indemnify for what type of digital loss. Generally, crime coverage covers theft of money or securities and can be expanded to cover BEC/EAC financial loss via a social engineering endorsement. Cyber insurance is available to cover breach-related expenses arising out of a cyber extortion, including the ransom demand, computer forensics costs and associated business disruption expenses or net income loss. Should that ransomware attack turn into a data breach, cyber insurance may indemnify for the associated costs of that as well, including liability costs, regulatory fines and penalties where insurable, as well as the costs of notification, public relations and credit monitoring.

Does the organization have a procedure to **verify new customers** prior to initiating any financial transaction?

The Corporation
THE PUZZLE

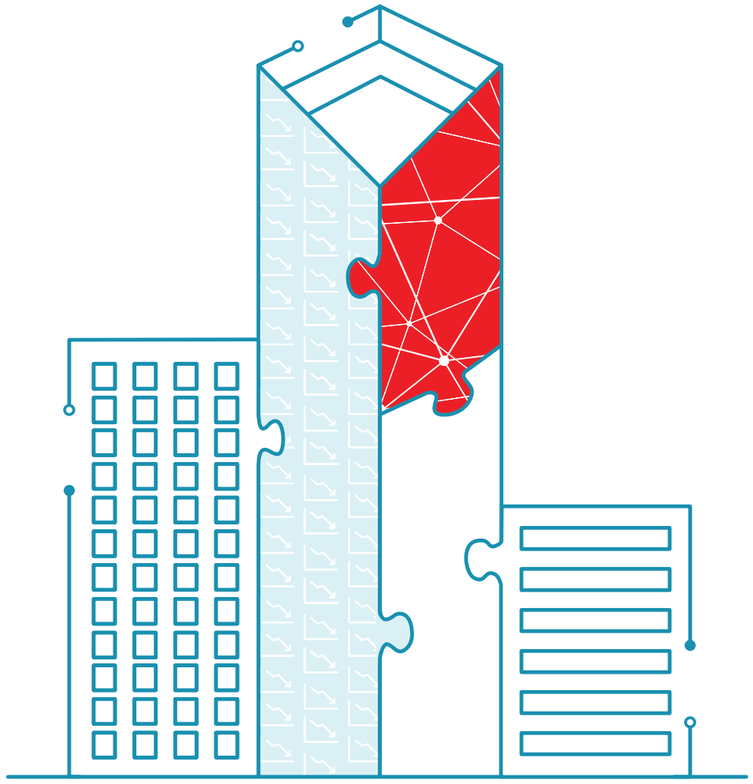
Cyber security and corporate liability risk are interwoven. In our **2019 Risk Report**, we discussed that the board of directors is increasingly liable for cyber security via fiduciary duties and companies risk facing class actions, regulatory fines and costs associated with investigations in response to cyber breaches.

A 2019 example is the securities class-action lawsuit brought against a shipping company and certain directors and officers, alleging that after a cyberattack, the company falsely assured investors that the impact on its newly acquired business was minimal and recovery was on track. Public companies are not only accountable to timely disclosure of cyber incidents, but also disclosure of risk, with the U.S. Securities and Exchange Commission (SEC) in 2018 directing public companies to take "all required actions to inform investors about material cyber security risks and incidents in a timely fashion." [35] This makes the puzzle ever more complicated.

The global cost of cyber security is reported to be almost $600 billion, or 0.8% of global GDP.[36] While there has not yet been a mega-settlements trend in response to significant breaches, the threat to the corporation is real, coming from many angles. Today, ratings outlooks are more reactive to the costs of a breach and investors look to ratings to determine the impact of a breach. One of the latest consequences for companies came in 2019, with the new risk of a ratings downgrade post data breach. A consumer reporting agency was the first organization in 2019 to see its outlook downgraded by Moody's in the wake of an attack. A ratings downgrade impacts the cost of capital, introducing direct ramifications to the organization's ability to execute strategic plans dependent on securing funds.

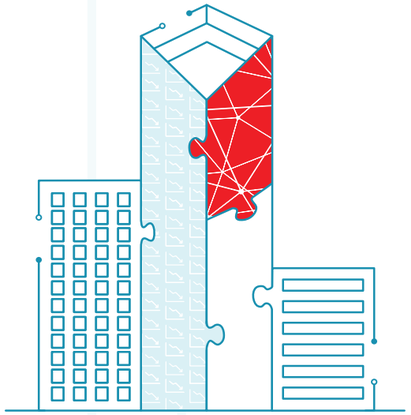
Though uncommon, bankruptcy is an unexpected yet plausible risk of a significant breach. In 2019, the parent company of a medical collection agency went from breach to bankruptcy filing in just two weeks. The compromised data included client information belonging to the collection agencies' customers, and as a result, various healthcare entities and service providers ended up disclosing the breach publicly. Along with an exodus of its client base and lost revenue, the investigation into the incident cost $400,000, and it cost an additional $3.8 million to send out the required notifications to seven million customers–that's over $4.2 million dollars in just reporting cost. In addition, there have been ensuing class-action lawsuits as well as scrutiny by state and federal regulators.[37]

Privacy remains a significant concern for companies from a corporate risk standpoint. In 2019, the first large fines were levied under the European Union's General Data Protection Regulation (GDPR) against a hospitality company and an aviation company, due to their 2018 data breaches. In January 2020, the California Consumer Privacy Act (CCPA) became effective, with California as the first U.S. state to introduce privacy regulations akin to the GDPR. It is broadly anticipated that other U.S. states will follow. Likewise, emerging as another piece in the corporate risk puzzle is the use of biometric data or any data related to human features. In 2008, Illinois became the first U.S. state to guard against the unlawful collection and storing of biometric information with the Biometric Information Privacy Act (BIPA). Additional states are passing similar legislation. In 2018 and 2019, 213 BIPA cases have been filed in Illinois state and federal courts. Most are class actions and directed at employers utilizing fingerprint technology for timekeeping purposes.[38]



Cyber security and **corporate liability** risk are interwoven.

The Corporation
THE PLAYBOOK



Cyber risk—as a form of corporate risk—is directly tied to balance sheet impact.

Companies should consider an organizational **assessment** and sensitive data mapping exercise to identify data that requires enhanced protection and governance, especially given the current environment of evolving (and increasing) global privacy regulation. Quantifying the financial impact of a cyber event is essential not only for good corporate governance, but also for strategic decision-making. A breach scenario **impact analysis** can bring needed visibility to guide investment decisions for information security, business continuity programs and risk transfer strategies.

Incident response readiness can help lessen the impact of a breach. An effective response can mitigate the potential reputational impact and liability from regulatory fines and penalties. This may be relevant in several ways, depending on the type of breach. It may demonstrate to regulators and shareholders that the company was prepared and that the directors and officers did not breach their fiduciary duty to the company. In the case of a credit card breach, it is important to have an independent forensic investigator to work with counsel to ensure that the PCI Forensic Investigator (PFI) reporting is accurate to minimize potential fines.

Robust **data protection and governance programs** should be established to include a holistic approach to identify, assess, protect, monitor and manage sensitive data throughout its lifecycle, regardless of where it is stored across the organization's operations. This will commonly require the integration of privacy compliance and cyber security initiatives and will typically employ various forms of technology, process and standards as well as policies across the organization.

Cyber breaches in recent years have led to investor scrutiny and event-driven litigation is a significant exposure for corporate leadership. **Insurance** can play a part in protecting companies from the liability associated with a breach. However, the insurance purchase for breach-related risk transfer is not one-size-fits-all. Directors' and Officers' liability insurance is vital to protect the corporation and the personal assets of the board against the costs of defending litigation and paying judgment awards or settlements. Other lines of coverage may come into play as well, such as employment practices liability coverage to protect against BIPA-related employment litigation. Cyber insurance is also an option for evolving privacy and security risks to protect companies against the financial statement impact of a breach, as well as provide pre-loss prevention and post-loss services, to help organizations to recover more quickly from the impact of a breach.

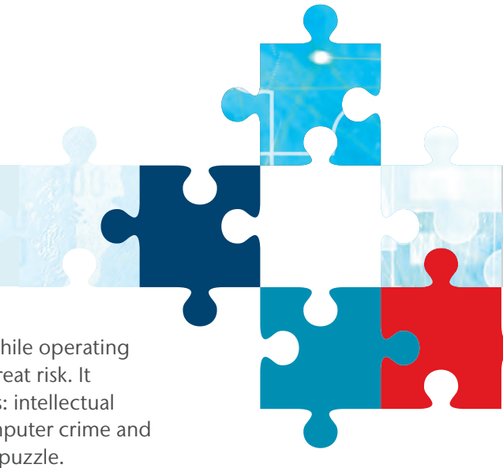
A breach scenario impact analysis can bring visibility to guide investment decisions.

2020

Taken together, the recommendations in this playbook have **one chief goal:**

To help enhance the organization's position against evolving cyber security risks and threats.

Putting It All Together



This playbook is designed to help organizations be successful while operating in a digital environment that presents great opportunity–and great risk. It pulls together thinking that considers less-publicized cyber risks: intellectual property, mergers and acquisitions, retirement, executives, computer crime and the corporation, adding these pieces to the evolving cyber risk puzzle.

Some of the plays to solve for cyber risk remain the same: stay informed, understand the organization's risk profile and be proactive in its defense. Others require more advanced action:

- √ Identify your organization's most critical data, dependent systems and business processes, and know where on the network they reside;
- √ Establish a sound incident response plan and put the plan into practice;
- √ Develop a regular cyber risk assessment program to track remediation progress and measure against evolving threats;
- √ Regularly test critical access points against cyber intrusion, especially new points of connectivity;
- √ Become deeply literate in risk transfer and understand what your portfolio of property and casualty insurance policies does or does not cover related to cyber security;
- √ Use financial modeling to quantify potential loss;
- √ Stay abreast of regulations and be aware that disclosing risk may be just as important as disclosing a breach;
- √ Realize the growing vulnerability of the executive team;
- √ Maintain a holistic cyber security program to include preventive, detective and reactive measures and controls, and mechanisms for continuous improvement.

Taken together, the recommendations in this playbook have one chief goal:
To help enhance the organization's position against evolving cyber security risks and threats.

Contributors

CYBER SOLUTIONS

Stephanie Snyder
Commercial Strategy Leader
stephanie.snyder@aon.com
+1 312.381.5078

Thomas E. Abel
Senior Vice President of Marketing and Business Development
thomas.abel@aon com
+1 212.903.2818

CJ Dietzman
Managing Director
cj.dietzman@aon.com
+ 1 212.903.2828

Chad Pinson
Executive Vice President Engagement Management — Cyber Security
chad.pinson@aon.com
+1 214.377.4553

Adam Peckman
Practice Leader–Cyber Risk
adam.peckman@aon.com
+1 201.856.9364

David Yaches
SVP, Corporate & Business Development
david.yaches2@aon.com
+1 212.981.2663

IP SOLUTIONS

Nick Chmielewski
Chief Broking Officer
nicholas.chmielewski@aon.com
+1 312.384.9881

FINANCIAL SERVICES GROUP

Chris Rafferty
Chief Operating Officer
chris.rafferty@aon.com
+1 312.381.4523

Cara LaTorre
Vice President & KRE Practice Leader
cara.latorre@aon.com
+1 212.441.2372

RETIREMENT SOLUTIONS

Robert Wilen
Senior Partner
robert.wilen@aon.com
+1 732.302.2169

Thomas W. Meagher
Senior Partner, Practice Leader
thomas.meagher@aon.com
+1 732.302.2188

M&A and TRANSACTION SOLUTIONS

Ian McCaw
Managing Director, Head of Cyber M&A
ian.mccaw@aon.co.uk
+44 (0) 20.7086.0561

William Shortt
Director of Cyber Diligence and Head of M&A Cyber Strategy
william.shortt@aon.com
+1 310.623.3272

Allyson Coyne
Managing Director & Senior Broking Officer
allyson.coyne@aon.com
+1 215.255.1715

Cyber Solutions Contacts

Jason J. Hogg
Chief Executive Officer
jason.j.hogg@aon.com

Eric Friedberg
Co-President
eric.friedberg@aon.com
+1 212.981.6536

Edward Stroz
Co-President
edward.stroz2@aon.com
+1 212.981.6541

AMERICAS

Christian E. Hoffman
President
christian.hoffman@aon.com
+1 212.441.2263

Brian Rosenbaum
Senior Vice President
brian.rosenbaum@aon.ca
+1 416.868.2411

LATAM

Temo Garcia
Senior Broker & U.S./Latin America Cyber Champion
temo.garcia@aon.com
+1 312.381.4398

EMEA

Onno Janssen
Chief Executive Officer
onno.janssen@aon.com
+49 (4) 03.605.3608

Vanessa Leemans
Chief Commercial Officer
vanessa.leemans@aon.co.uk
+44 (0) 20.7086.4465

APAC

Michael Parrant
Cyber Insurance Practice Leader
michael.j.parrant@aon.com
+6 (141) 333.9783

Andrew Mahony
Regional Director
andrew.mahony@aon.com
+6 (58) 428.1965

References

1. "2019 Intangible Assets Financial Statement Impact Comparison Report," Aon plc and Ponemon Institute, 2019.
2. "The Commission on the Theft of American Intellectual Property," The IP Commission, 2018.
3. "2019 Intangible Assets Financial Statement Impact Comparison Report," Aon plc and Ponemon Institute, 2019.
4. https://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm.
5. "Apple has 'deep concerns' that ex-employees accused of theft will flee to China," Stephen Nellis, Reuters, 2019.
6. "UPDATE 1-Australian metal detector company counts cost of Chinese hacking," Reuters, 2015.
7. "The Board Ultimatum: Protect and Preserve.The rising importance of safeguarding trade secrets 2017," Baker McKenzie and Euromoney Institutional Investor Research, 2017.
8. "The Board Ultimatum: Protect and Preserve.The rising importance of safeguarding trade secrets 2017," Baker McKenzie and Euromoney Institutional Investor Research, 2017.
9. "IP Within the Boardroom, Is intellectual property a director and officer issue?" Ethical Boardroom Magazine, 2019.
10. "M&A and Transaction Solutions: Risk in Review," Aon plc, 2018.
11. "Top Five Cyber Risks in Mergers & Acquisitions," by Ian McCaw, Aon plc, via LinkedIn, 2019.
12. "Marriot Faces GDPR fine of 123 million," Forbes, 2019.
13. "Verizon knocks 350m off yahoo sale after data breaches," TechCrunch, 2017.
14. "M&A and Transaction Solutions: Risk in Review," Aon plc, 2018.
15. "North America M&A and Transaction Solutions: Risk in Review," Aon plc and Mergermarket, 2019.
16. "Asia-Pacific M&A and Transaction Solutions: Risk in Review 2019," Aon plc, 2019.
17. "Retirement Plans Incur Data Breaches; ERISA Council Addresses Cyber Risks," McGuire Woods, 2016.
18. "Custodian's cyber fallout with pension fund is a wake-up call," Anna Reitman, Securities Finance Monitor, 2019.
19. "2019 Global Pension Risk Survey," Aon plc, 2019.
20. "The ERISA Advisory Council Asks DOL for Guidance on Cybersecurity," Lee Barney, plan adviser, 2018.
21. "Suit against Estée Lauder spotlights 401k Distribution Fraud," Paul Roberts, The Security Ledger, 2019.
22. "Data Breach Risks for 401(k) and Retirement Plans," Jones Day Alert, 2017.
23. "2019 Data Breach Investigations Report," Verizon, 2019.
24. "2019 Data Breach Investigations Report," Verizon, 2019.
25. "2019 Data Breach Investigations Report," Verizon, 2019.
26. "Aon Risk Solutions High-Net Worth Cybersecurity Survey," Aon plc, 2018.
27. "2019 Data Breach Investigations Report," Verizon, 2019.
28. "C-Suite Perspectives: From Defense to Offense – Executives Turn Information Security into a Competitive Differentiator Report," Radware, 2019.
29. "Internet Crime Report," United States Federal Bureau of Investigation, 2018.
30. 2018 Association of Certified Fraud Examiners (ACFE) Report to the Nations, 2019.
31. "Internet Crime Report," United States Federal Bureau of Investigation, 2018.
32. "Business Email Compromise: Three Real Case Studies," First Bank, 2019.
33. "2019 Cybersecurity Almanac," Cisco and Cybersecurity Ventures, 2019.
34. "Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up," Krebs on Security, 2019.
35. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," U.S. Securities and Exchange Commission, 2018.
36. "Economic Impact of Cyber Crime: No Slowing Down," CSIS and McAfee, 2018.
37. "AMCA Bankruptcy Filing in Wake of Breach Reveals Impact," Bank Information Security, 2019.
38. "BIPA Update: Class Actions on the Rise in Illinois Courts," Holland and Knight, 2019.

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Visit aon.com/cyber-solutions for more information.

Empower Results®