paloalto NETWORKS

CRYPSIS A PALO ALTO NETWORKS COMPANY

2020 INCIDENT RESPONSE & DATA BREACH REPORT

CORTEX BY PALO ALTO NETWORKS

paloaltonetworks.com | crypsisgroup.com

CONTENTS

3 FOREWORD

4 EXECUTIVE SUMMARY

7 METHODOLOGY

8 VERTICAL SECTOR REPORT CARD: THE HARDEST HIT SECTORS, 2019

11 RANSOMWARE

12 Initial Attack Vector

13 Ransomware Variants

15 Ransom Payment Trends

16 Advancing Techniques: Threat Actor Methodology Changes

17 Navigating the Maze

18 Ransomware: Vertical Sectors

19 Act Now: Ransomware Prevention Pro Tips

23 BUSINESS EMAIL COMPROMISE

24 BEC and Sensitive Data Exposures

24 Threat Actor Intent

26 BEC: Vertical Sectors

28 Act Now: BEC Prevention Pro Tips

29 Importance of Cyber Insurance

30 DATA BREACHES

30 Network Intrusions

30 Web Application Compromise

31 Payment Card Breaches

32 Advanced Persistent Threat (APT) Nation State Attacks

34 Act Now: Network Intrusion Prevention Pro Tips

36 Inadvertent Disclosure

37 Top Cause of Inadvertent Disclosure Events in 2019

38 Inadvertent Disclosure: Vertical Sectors

40 Sensitive Data Exposure

41 Act Now: Inadvertent Disclosure Prevention Pro Tips

43 Insider Threats

44 Threat Actor Intent

45 Attack Methodologies

46 Insider Threats: Vertical Sectors

48 Act Now: Insider Threat Prevention Pro Tips

50 ABOUT THE CRYPSIS GROUP

FOREWORD

By General Michael Hayden

An unfortunate and never-ending war is being fought on the front lines of cyberspace. Nation state actors are much better equipped and trained for battle; however, many who would otherwise be noncombatants are required to take up arms to fend for themselves. While this war is invisible to most and fought in the realms of the vast and indefensible internet, the costs are tangible and truly astronomical—cybercrime is everyone's problem and a risk to every business, an ominous specter that can't be fully subdued.

What's the answer? How do we win the war on cybercrime? While we often look to the government to take the lead in the face of such threats, much of this battle is and must be fought by private sector businesses with all their ingenuity, autonomy, and innovation. Cyber threats evolve at an alarming pace; and I believe that, in this case, the private sector—including the businesses that must employ security governance, policies, controls, and best practices, as well as the cybersecurity firms charged with assisting and advising them—must lead the way, arming themselves against the barrage of attacks. The government's role should be to offer support and resources in the quest to better overall security.

General Michael Hayden is a retired four-star United States Air Force General, the former Director of the Central Intelligence Agency (CIA), and the former Director of the National Security Agency (NSA). He is a globally recognized expert in security, intelligence, and global terror and cyber risks.

Knowledge, as has historically always been the case, must be leveraged to arm the defenders. When we understand the threat, we can devise a strategy to mitigate it. This report by The Crypsis Group provides an assessment of today's threats in the cybersecurity battlefield and the countermeasures companies can employ to better protect themselves.

What becomes clear from its pages is that the problem is extremely complex; yet the solution is, in part, "back to the basics": rigorously following cybersecurity best practices across the entire digital ecosystem, from endpoints to third-party providers. And, knowing when you need help, calling in experts to help when an incident occurs or beforehand, to avoid one in the first place.

Cybercrime isn't going away any time soon. It's not a war with a defined end—it's an ongoing, rigorous grind that requires diligence, care, and expertise. Suit up, dig in, and keep up the fight.

EXECUTIVE SUMMARY

By Bret Padres

After many years of helping clients respond to cybersecurity incidents, we continue to be amazed at the diversity of cyber threats and the creativity, innovation, and adaptability of threat actors. Our investigations reveal the intricacies of how these attacks have evolved to stay just ahead of the adoption of organizational cybersecurity defenses. As long as there are ways to profit from cybercrime, threat actors will continue to find new methods to exploit vulnerable systems and processes.

Our amazement should not be mistaken for admiration. We know all too well the destruction these incidents cause as we work every day to help organizations respond and recover. Recent attacks on healthcare institutions and supporting organizations during the worldwide coronavirus pandemic serve as a stark reminder that these attacks—while waged from a keyboard—are crimes, and the threat actors remorseless.

In this report, we analyze data and leverage insights from over 1,000 investigations The Crypsis Group conducted in 2019, ranging from ransomware, business email compromise (BEC), payment card breaches, and nation state attacks, to inadvertent data disclosure incidents and insider threat investigations. Our intention is not to criticize those charged with protecting information technology assets, but rather to offer rich, deep insights into real-world cybersecurity risks and, importantly, provide practical advice on how organizations can protect themselves. We present this data within commonly encountered incident types and discuss the interconnected nature of attacks within each.

> As long as there are ways to profit from cybercrime, threat actors will continue to find new methods to exploit vulnerable systems and processes.

BELOW IS A SUMMARY OF THE KEY INSIGHTS DERIVED FROM THIS REPORT

Here is how organizations were most likely to be hacked in 2019.

Ransomware attacks and BEC continue to be among the most pervasive and impactful cyber threats to organizations in terms of business disruption and monetary loss.

- Ransomware and BEC represent public enemy number one and two, respectively, as well as the most common reasons why Crypsis was retained to help organizations respond to cyber attacks.
- If you're a threat actor, there is simply no better way to monetize illicit access to a network than encrypting your victims' files and demanding payment.
- Email systems provide a wide attack surface and target-rich environment, with access to financial transaction details and/or other sensitive data only a few clicks away.

Health, wealth, and cybercrime: The top targeted industries were Healthcare and Financial Services.

- Compared to other industry sectors, Healthcare and Financial Services organizations store, transmit, and process high volumes of monetizable sensitive information that disproportionately attract threat actors.
- Sixteen percent of all incident response matters we handled in 2019 were with healthcare-related businesses.
- Financial Services was the second most targeted sector, taking 14% of our share of security incidents.

Ransom who, what, and "ware": Ransomware monetary demand amounts are trending up; threat actors have evolved, are employing more sophisticated tactics, and are adding data exfiltration and extortion to the mix.

Since 2018, threat actors have evolved from deploying mass-distributed phishing campaigns with lower ransom demands to highly targeted, well-researched attacks on larger enterprises with deeper pockets.

- Requested ransom amounts rose nearly 200% from 2018 to 2019, averaging $115,123 in 2019.
- The Healthcare sector was the most affected (22% of our 2019 ransomware matters), with the Manufacturing sector coming in second (13%).
- More incidents have included the deletion or disablement of backups, as well as the threat of releasing sensitive data publicly. The threat actor group known for deploying the Maze ransomware is leading the way in extortionate tactics, but others are getting into the game.
- We believe these new methods represent a tactical shift in response to stronger enterprise security defenses and an associated reduction in organizations' willingness to pay.

Continued on next page >

KEY INSIGHTS *(continued)*

BEC—because they can: Threat actors continue to capitalize on organizations' migration of enterprise email to the cloud.

BEC attacks primarily leverage phishing—preying on the vulnerabilities of humans—to harvest cloud-based email passwords with the intent of committing wire fraud.

- Across all incident types, one third of our overall matters in 2019 were BEC attacks.
- In nearly all cases, the motive of the attack was wire fraud, with an average theft of wired funds per incident of $264,117 in 2019.
- Financial Services and Healthcare sector organizations were the hardest hit, due, we believe, to their high volume of financial transactions and reliance on email to conduct them.
- Nearly half of the BEC incidents we investigated in 2019 involved the unauthorized access to, or exfiltration of, sensitive information.

Insider threats were the dark horse cyber risk of 2019.

While nation state and e-crime threat groups garner the headlines, insidious insiders are silently grabbing our sensitive data. These threats are often overlooked and deserve more focused attention.

- Our insider threat investigations rose approximately 70% year over year.
- In terms of motive, 57% of attacks were waged by employees looking to advance their careers and who were departing the victim organization, whether or not the organization was aware of the employee's impending departure.
- In our observation, the IT security function within organizations focuses more time and resources on external threats than on internal ones, leaving sensitive data exposed to those who have authorized access and malicious intent.

Great plans still fail: Attackers capitalizing on organizations' inadvertent disclosure of data was the source of the largest volume of sensitive data compromise.

Inadvertent disclosure—such as accidental cloud misconfigurations—often results in highly impactful sensitive data compromise once attackers pick this low-hanging fruit. Inadvertent disclosure incidents often involve high-volume databases, exposing large repositories of sensitive data.

- These events exposed 713,000 individuals' records on average per incident (vs. 9,400 on average per incident in BEC cases).
- 45% of our inadvertent disclosure investigations involved sensitive data.
- We believe that complexities of emerging cloud technologies, together with an organizational inability to manage that complexity, is fueling this trend. All told, we see these incidents resulting from small and mid-sized organizations struggling to find the expertise required to manage this complexity, and larger enterprises grappling with the excessive scale and scope of the problem.

We hope you find the contents of this report illuminating and the pro tips helpful in your quest toward greater security.

METHODOLOGY

This is a descriptive baseline report informed by a study of data and learnings from over 1,000 incidents The Crypsis Group responded to in 2019. We reference data from 2018 through 2020 where helpful to understand longer-term trends. Though this is one view of the global data breach landscape, these matters are representative of broader threat trends and supported by deep empirical insights from our experienced investigators. All sizes of companies, vertical sectors, and a range of geographic regions are represented.

While The Crypsis Group engages in a broad range of services (extending to proactive cybersecurity services and expert witness testimony), the report is structured to focus on security "incidents," "matters," or "cases" (used synonymously)—actual and suspected data breaches, data exposures, or malicious threat actor intrusions for which we are called in to investigate—while leaning heavily on our experience in our other cyber-related service areas. We follow the common cybersecurity industry practice of considering a "breach" to be an incident that results in the confirmed disclosure of data to an unauthorized party. Throughout this report, we reference "breach determinations" and "data exposures" to refer to investigations where a determination was made that a breach was possible or likely. As an incident response firm, we conduct our forensic investigations to determine whether a breach occurred, or whether one may possibly have occurred, given findings of unauthorized access to a system or account.

The report is structured around the following incident categories:

- Ransomware
- BECs
- Data Breaches, including:
  - Network Intrusions (Web Application Compromises, Payment Card Breaches, and APTs)
  - Inadvertent Disclosure
  - Insider Threats

Although ransomware and BECs may in many cases be considered data breach matters, we have dedicated sections of this report to these respective threats and pro tips for mitigation due to their pervasiveness. Each threat category is defined and covered in full within the pages to follow.

VERTICAL SECTOR REPORT CARD

THE HARDEST HIT SECTORS, 2019

Healthcare wins the dubious distinction of being the most targeted sector of 2019, drawing from our data across all incident types. Sixteen percent of all incident response matters we handled in 2019 were with healthcare-related businesses (including healthcare delivery organizations, healthcare device manufacturers, and technology providers; see Figure 1).

- Ransomware was the attack type of choice against healthcare organizations in 2019—they suffered more ransomware attacks than any other kind and represent a significant 22% of all our ransomware cases in 2019.
- Healthcare organizations were also hit hard with BEC attacks, representing 15% of observed incidents, and also with insider threat and inadvertent disclosure incidents (16% and 15%, respectively).

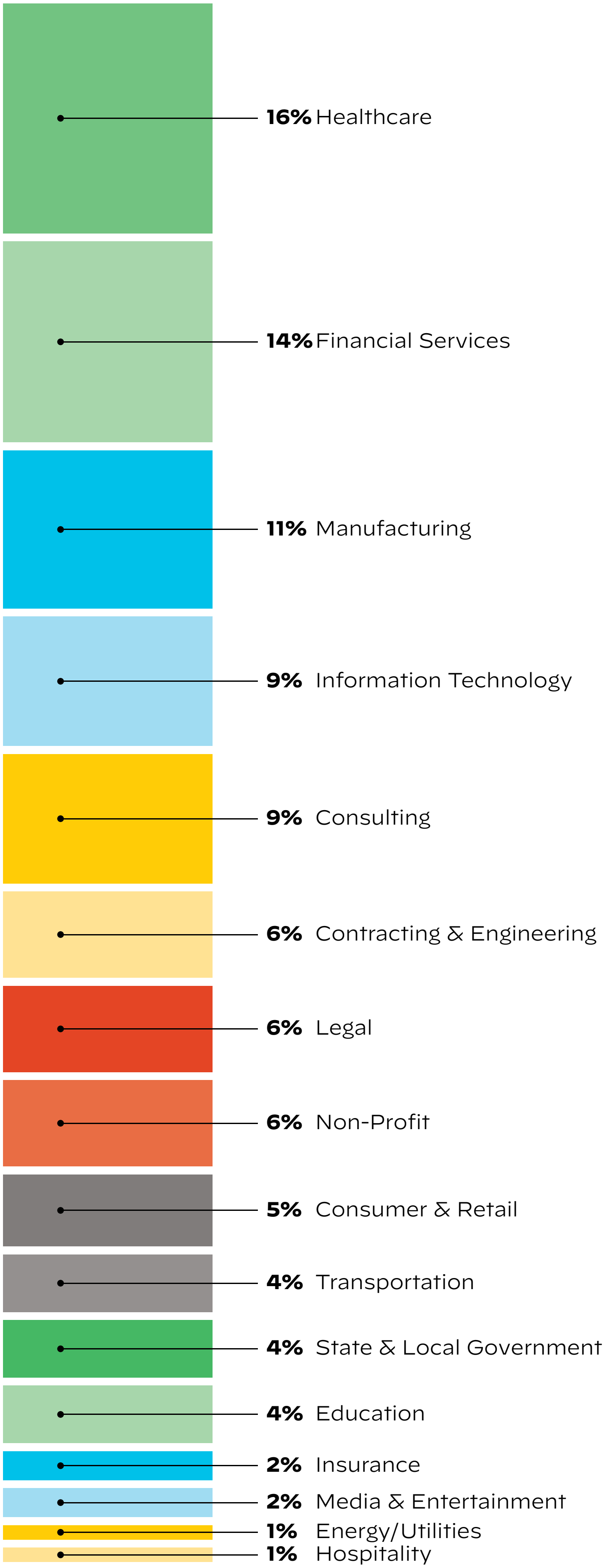


Figure 1: Distribution of all incidents in 2019 by vertical sector

> Compared to other industry sectors, healthcare and financial services organizations store, transmit, and process high volumes of monetizable sensitive information that disproportionately attract threat actors.

Financial Services was the second most targeted sector, taking 14% of our share of security incidents.

- Our Financial Services customers suffered most from BEC attacks; nearly 18% of all BEC cases in 2019 were within this sector.
- Financial Services also fared poorly in the insider threat category (16% of our cases) and in inadvertent exposure incidents (17%).

The Information Technology sector accounted for the highest number of inadvertent disclosure incidents, at 18% of our data set. These companies also saw a comparatively higher number of insider threat cases.

Manufacturing was a frequent victim of ransomware in 2019 (accounting for 13% of our ransomware matters), most frequently with the Ryuk variant, likely due to the fact this variant's actors use well-researched phishing attacks that result in a higher success rate. This sector also saw a relatively high number of BEC attacks (10% of these matters).

Consumer & Retail, along with Information Technology, were the prime recipients of payment card attacks. While the Payment Card Industry (PCI) Security Standards Council has accomplished much in recent years to provide card data protection guidelines, threat actors continue to find new methods to target this data.

The remainder of vertical sectors in our sample, including Legal, Energy & Utilities, Consulting, and others, may not have taken the lion's share in any one attack category, but they did experience incidents across every threat type. A common theme we have seen is that smaller organizations across all sectors are frequently targeted. More on this follows.

VERTICAL SECTOR REPORT CARD: THE HARDEST HIT SECTORS, 2019

We conclude, both from our data herein and insights with these matters, that the frequency and types of incidents vertical sectors experience are a combination of factors, including:

The value of the data they control and maintain.

For the same reason Willie Sutton stated he robbed banks ("Because that is where the money is"), organizations that are known to store, transmit, and process broader spans of monetizable data can disproportionately attract threat actors. Healthcare and Financial Services are two such examples. Information Technology, which often includes Cloud Services Providers (CSPs) that host large databases, also fall into this bucket. Other data of value can include intellectual property and payment card data, which can be either monetized or used for personal advantage (such as we see in insider threat cases).

The perceived security posture of the vertical sector.

Small to mid-sized businesses (SMBs) of all types and specific sectors like Healthcare are generally considered to be lacking in defensive security sophistication and can receive more attacks—the perception tends to lead to over-targeting of this group.

The actual security posture of the organization.

Much of our work is dedicated to determining incident root cause. We find the root cause often points to the fact that smaller organizations have fewer dedicated staff to find and resolve security incidents. On the other end, much larger organizations have more resources, but deal with a vast, constantly evolving technology and threat landscape.

The criticality of ongoing operations.

Ransomware threat actors benefit from the universal reliance of a business on one of its most critical assets—its data. They take hold of the victim's data without having to remove it from the environment or even understanding anything about the data itself. As we present within this report, these threat actors have become more targeted and are selecting victims that are likely to be compelled to pay because of the high availability requirements of their operations. In organizations like hospitals and managed service providers, urgency in restoring ongoing operations is one factor in risk.

RANSOMWARE

In the decades that followed the creation of the very first documented ransomware variant in 1989—the AIDS Trojan, developed by Harvard trained Joseph Popp, who strangely distributed the malware through the postal service via floppy disk—ransomware has become a persistent, business-disabling, and costly challenge. Ransomware is a type of malware designed to deny access to a computing system or data (usually via encryption) until a ransom is paid.

More recently, ransomware threat actors have also used the threat of data publishing as leverage to extract payment. Its spread exploded with the rapid growth of the internet and was fueled by the emergence of cryptocurrency in 2009. The rise of bitcoin and other cryptocurrencies gave threat actors an efficient and anonymous method to extract ransom from victims while hiding their trail. Since 2015, ransomware attacks on organizations and municipalities have appeared to increase considerably; yet, their acceleration is difficult to accurately quantify. Many organizations do not disclose ransomware attacks. The costs to businesses, however, are real and rising: According to a prediction by

TOP THREE PRO TIPS TO PREVENT RANSOMWARE ATTACKS

1

Patch all of your organization's systems as quickly as possible to prevent vulnerability exploitation.

2

Conduct employee security and phishing prevention training.

3

Disable direct external Remote Desktop Protocol (RDP) access.

Read a detailed list of ransomware prevention pro tips on page 21.

Cybersecurity Ventures,[1] global ransomware damages are forecasted to reach $20B by 2021, vs. the estimated $325M in damages in 2015. The Crypsis Group has assisted hundreds of clients with ransomware incidents in 2019 alone, attesting to this tactic's broad reach. In the past year, we have witnessed attackers target multinational corporations, state and local governments, healthcare organizations, and even small businesses such as bowling alleys, grocery stores, and tax accountants, impeding each organization's ability to conduct business or serve their communities until fast and effective response measures are taken. This speaks to the core of the attackers' tactics: ransomware threat actors know that many organizations cannot afford even short disruptions in core business operations, providing a strong incentive to pay.

The landscape is evolving rapidly, with cybercriminals constantly innovating to find new techniques to exploit victims for financial gain.

Initial Attack Vector

In Crypsis's 2019 data set, the number one initial attack vector was through **RDP services,** occurring in 50% of our ransomware matters. This has been a consistent trend in our investigations from 2018 to present. When enabled, RDP allows users to remotely connect to other Windows-based devices or networks; it is commonly used by IT service providers or remote workers. Implementing RDP without adequate controls can leave systems vulnerable to attack. For example, weak passwords, unrestricted internet access, unlimited authentication attempts, and using outdated RDP protocols can all leave the door open to threat actors. Remote workers, largely those from SMBs that do not employ adequate protections (though the risk is certainly not limited to SMBs), can be compromised by attackers that scan for such exposed systems and then exploit them.

The second leading attack vector for all organizations in 2019 (found in 43% of our ransomware matters) was **social engineering,** typically a phishing or spear phishing email attack. Social engineering exploits human behavior: a threat actor manipulates the victim into taking some action that allows the threat actor access to an organization's network or data. This most often occurs by inducing the victim to provide their password into a malicious web form—a method known as "credential harvesting."

Web application attacks against external-facing systems was our third top attack vector in 2019 (7% of our matters). Here, the threat actor relies on exploiting vulnerabilities in internet-facing applications to compromise the victim. Preventing these attacks can be difficult, as it requires comprehensive knowledge of all deployed frameworks and dependencies, along with a robust vulnerability management program to keep systems up to date. Additionally, mitigation technologies, safeguards to control internet-facing applications, and a security operations function to provide ongoing detection and response can help prevent these attacks.

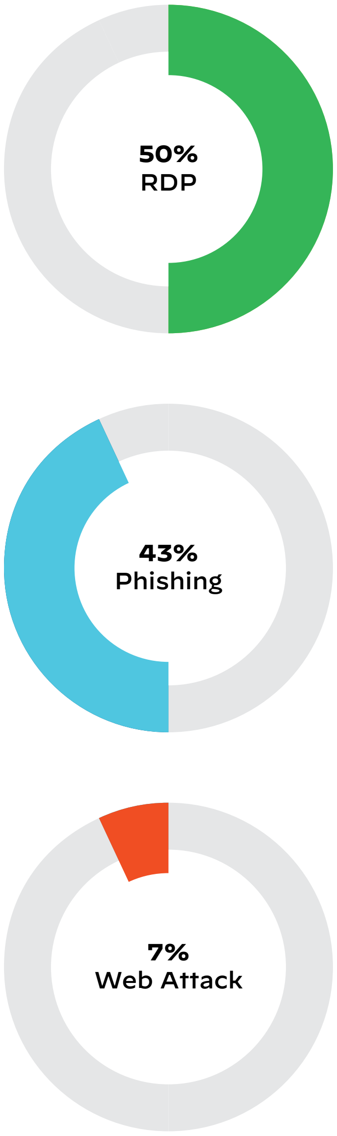


Figure 2: Most common attack vectors seen in 2019 ransomware incidents

[1] Steve Morgan, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, Cybersecurity Ventures, (Oct. 21, 2019), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.

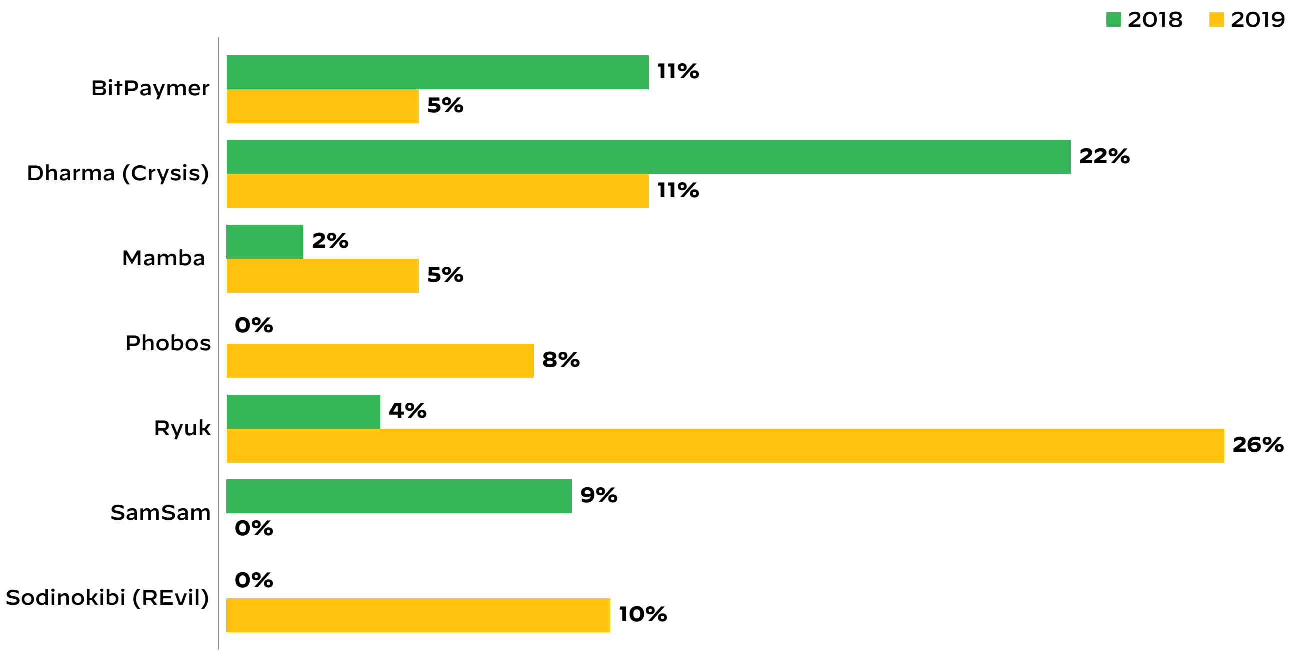


Figure 3: Variants as a percentage of cases, 2018 vs. 2019

Ransomware Variants

In the past few years, we have observed the wax and wane cycles of the variants used in ransomware attacks and how these variants correspond with changing ransom trends and tactical approaches. In 2017/18, malware families like Dharma (also called "Crysis") and SamSam were seen most commonly in our investigations. The use of these variants fell by the end of 2018 as threat actors adopted new tactics and ransomware to force payments from their victims.

2019 saw the rise of ransomware variants Ryuk, Sodinokibi (also called "REvil"), and Phobos. These variants and the adversarial tactics surrounding them are highly effective and escalated quickly over the year.

Phobos, a variant nearly identical to Dharma, came on the scene in early 2019. While it is believed that Phobos was created by the same threat group that created and executed Dharma ransomware, the threat actor's branding and tactics differ. While Dharma was more often used with what are known as "spray and pray" tactics, Phobos is used in targeted attacks.

Like Phobos, Sodinokibi also appeared at the beginning of 2019. It is widely believed that Sodinokibi is related to GandCrab, a previously prolific ransomware variant seen in 2017 and 2018. Compared to other ransomware families, Sodinokibi is unique in how quickly it has evolved. Over the course of 2019, Sodinokibi was improved several times, becoming harder to detect and more resistant to reverse engineering efforts.

Ryuk ransomware, which first appeared in 2018, was the most common variant observed by Crypsis in 2019. It has been dangerously effective over the past year, in part due to the initial attack tactic used by the threat actors. Threat actors behind Ryuk are utilizing a banking trojan called TrickBot to release effective spam/phishing campaigns against victims. This is the first time Crypsis analysts have observed a ransomware so closely correlated with banking data theft attacks.

The development of sophisticated adversarial tactics used in conjunction with the ransomware makes attacks with these variants increasingly effective.

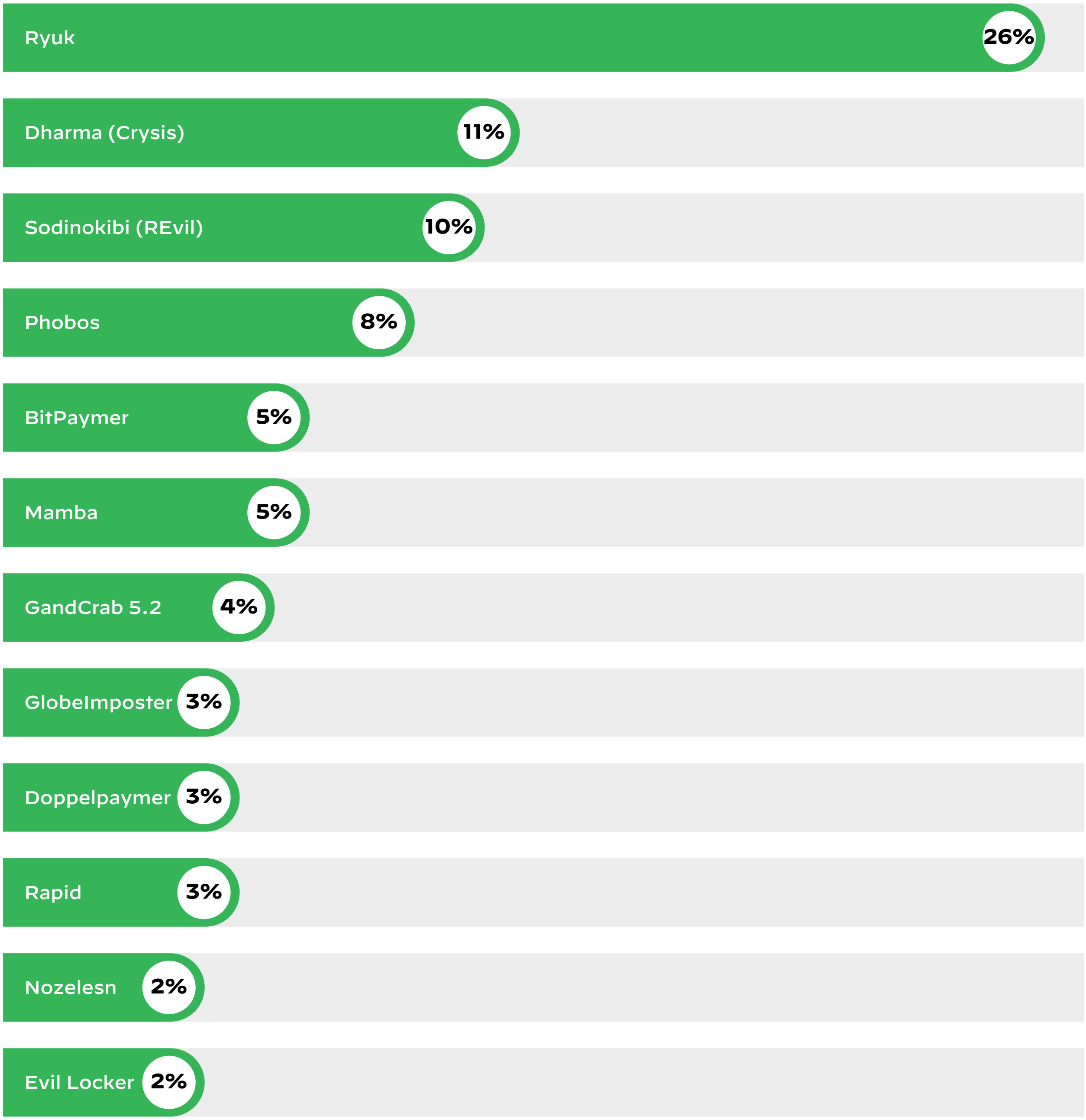


Figure 4: Most common ransomware variants used in 2019 (by percentage of cases)

Ransom Payment Trends

It is no surprise to us that attackers are demanding exorbitant ransoms. In the past three years, Crypsis observed the following trends:

- **Average requested ransom amounts rose 200% from 2018 to 2019, averaging $115,123 in 2019.** This is due in part to the shift toward attackers' use of enterprise-targeted ransomware families and careful selection of victims capable of paying higher sums, as well as the maturing tactics we will discuss later in this report. Cybercriminals, in their determination to be paid, use every approach in their arsenal to earn maximum return from each attack. In 2019, Crypsis particularly observed Ryuk and Sodinokibi variants driving average ransom payments significantly higher. Earlier variants like Dharma and LockCrypt resulted in much lower ransom demands of around $17,707 on average in 2017 and 2018.
- **The highest ransom paid since 2015 in a Crypsis matter was $5M:** paid by an organization in the Healthcare sector.
- **The highest ransom demanded in a Crypsis matter since 2015 was $15M,** demanded of a data center and solutions provider victim.

The median ransom payment has grown even more dramatically since the beginning of 2018, increasing 300% from the first quarter of 2018 to the last quarter of 2019. The rise in both median and average ransom demand is, in our analysis, attributable to changing tactics and methodologies that grew in response to defensive actions taken by organizations, as explored in the following section.

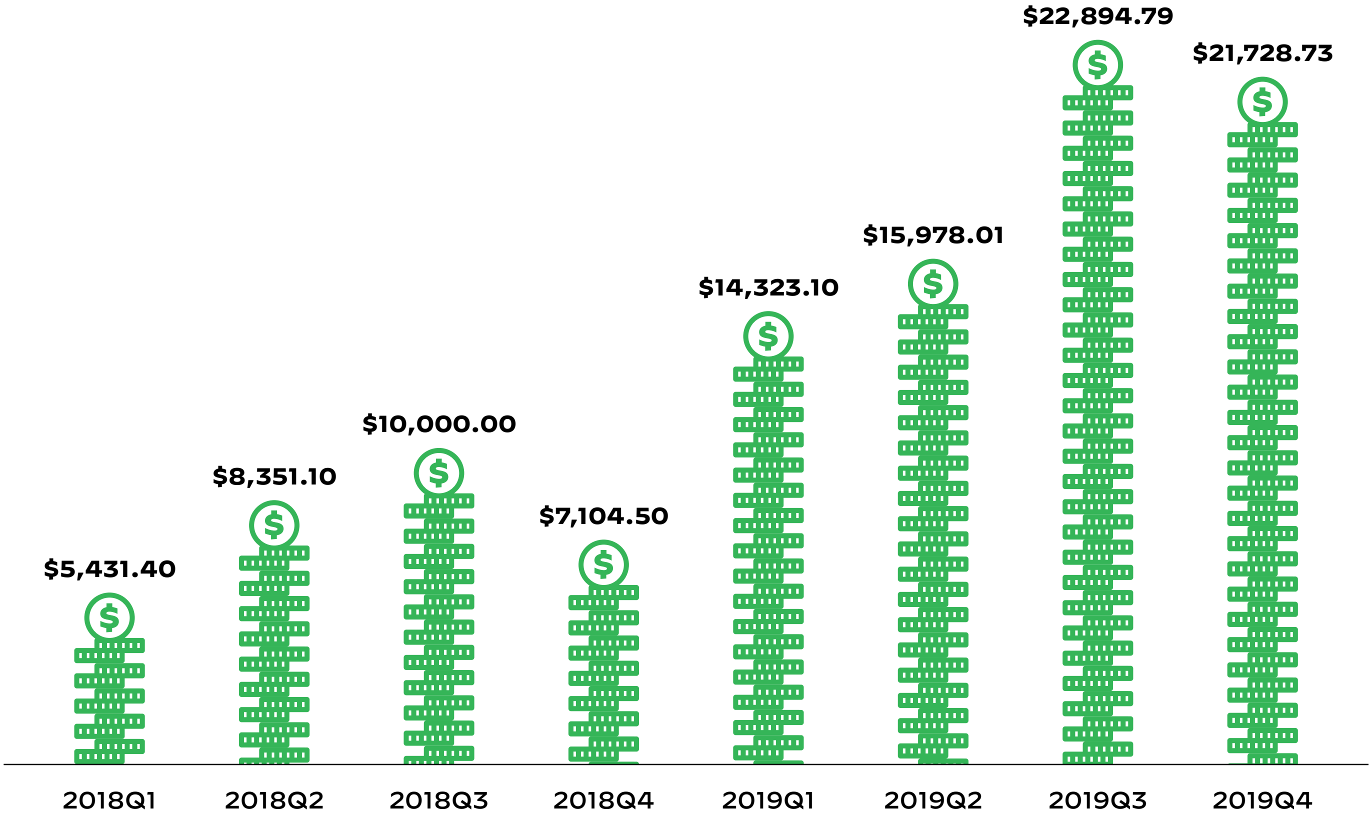


Figure 5: The rise in median ransom demanded payments (USD), from 2018–2019

Advancing Techniques: Threat Actor Methodology Changes

In the early days of ransomware, we observed threat actors attempting to strike as many victims as possible in a single campaign. Known as the “spray and pray” method, attackers used mass-phishing emails to try to reach as many people as possible to increase their click rate, victim count, and total ransoms earned with minimal time investment. Their approach was victim-agnostic, targeting individuals and organizations in all vertical sectors. Because it was lucrative, costs to victims began to rise rapidly as more threat actors adopted ransomware as their attack method of choice.

The costs incurred from both ransomware and other cyberattack modalities (including both monetary and reputational damages) appear to have had some net-positive effect: organizations began to take more proactive steps to reduce risk, prioritizing information security monitoring, and developing cyber risk management programs. In 2015, the global cybersecurity market was estimated at $75B;[2] in 2018, it grew to an estimated $118.78B.[3]

In the past one to two years, we have observed threat actors adopting new tactics in every step of the attack; in response, we believe, to the reduced effectiveness of the older, indiscriminate campaigns, attributable in part to an improved enterprise security defense posture.

Armed with new technology and a more targeted approach, threat actors have been increasingly tactical in their victim selection. From our conversations with threat actors during ransom negotiations, we have become aware of lengthy due diligence on victims. Tactics include reviewing and researching an organization’s U.S. Security and Exchange Commission (SEC) filing documents, public website, social media, and executive information to ensure an organization’s ability to pay. After targeting and successfully breaching the targeted company, the more sophisticated threat actor then takes time in ensuring they understand their victim’s technology landscape to increase the likelihood that full disruption will occur.

Most recently, Crypsis has noted threat actors taking things one step further. Extortion. Let’s talk about Maze.

From late 2018 through 2019, Crypsis observed threat actors:

- Finding and disabling or deleting system backups
- Identifying the number of endpoints connected to the system
- Whitelisting their ransomware with the victim’s security tools to ensure the attack will be as devastating and as far reaching as possible
- Uninstalling antivirus software
- Being less willing to negotiate ransoms, using knowledge of company financials to deny reduced ransom offers
- Selling ransomware-as-a-service (RaaS) to other or less advanced threat actors, giving them quick access to a wider range of victims

[2] Steve Morgan, *Cybersecurity Market Reaches $75 Billion In 2015 ; Expected To Reach $170 Billion By 2020*, Forbes, (Dec. 20, 2015), https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#cb6831130d60.

[3] Mordor Intelligence LLP, *Cyber Security Market — Growth, Trends, and Forecast (2019–2024)*, ReportLinker, (Oct., 2019), https://www.reportlinker.com/p05826213/Cyber-Security-Market-Growth-Trends-and-Forecast.html?utm_source=PRN76.

Navigating the Maze

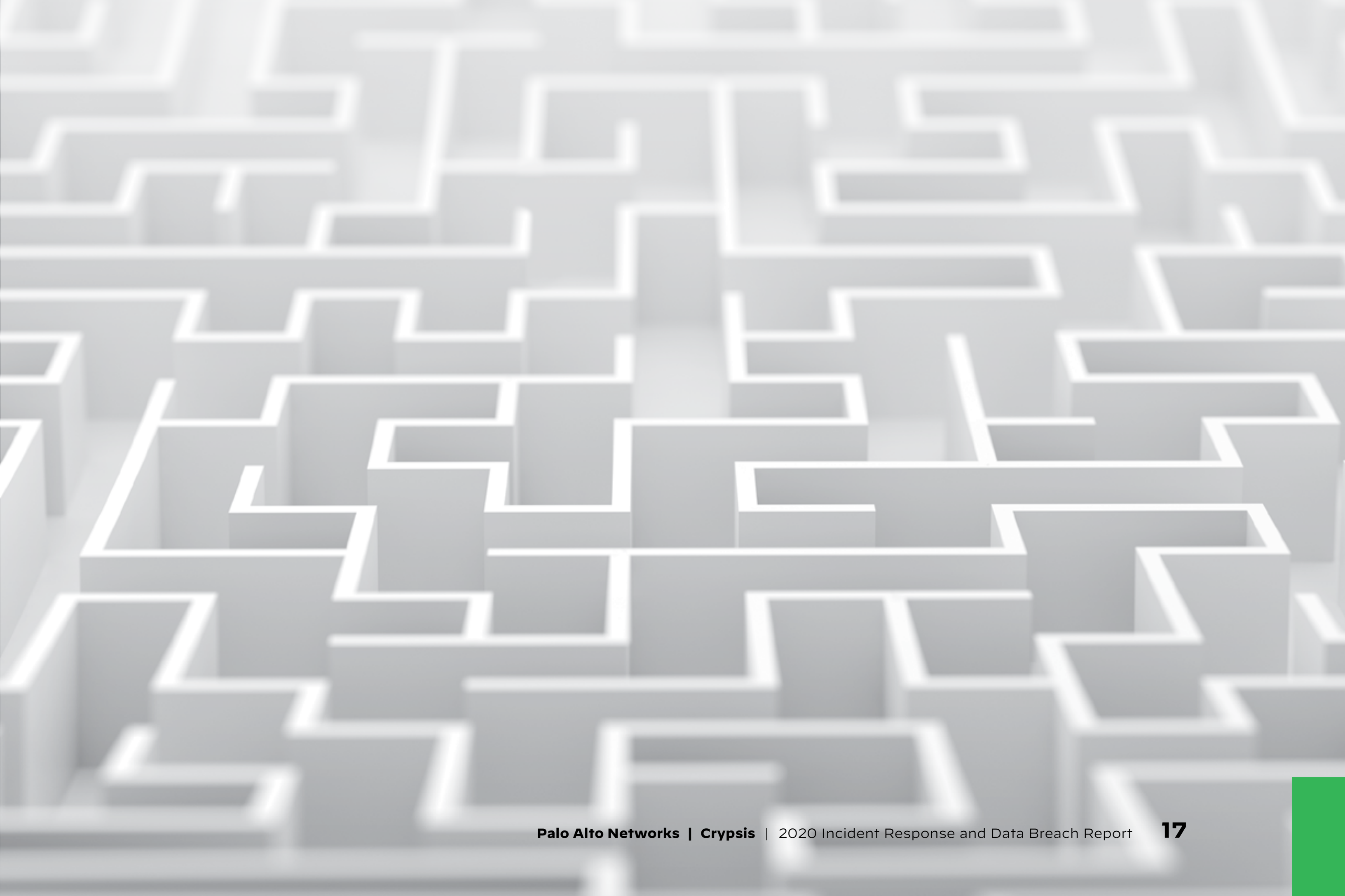
Crypsis first observed Maze ransomware in late 2019. Similar to Ryuk, threat actors using it appeared to be targeting large organizations with higher ransom demands than we had typically seen. However, the threat actors behind Maze have added extortion to the mix: threatening to post the victim's exfiltrated sensitive data on a public website designed for this purpose.

This is a significant shift. Prior to the introduction of Maze, Crypsis's forensic analysis of ransomware incidents rarely found evidence of data exfiltration, sparing victims the burden of a notifiable event.

> The threat actor group known for deploying the Maze ransomware is leading the way in extortionate tactics, but others are getting into the game.

Other threat groups are starting to follow suit, widening the wake of damage ransomware causes to include reputational harm when sensitive information is made public. In 2019, 4% of Crypsis's ransomware resulted in a breach determination—still a small population, but an indication of the growing trend toward more extortionate methods used by Maze and other threat actors.

One of the silver linings of ransomware incidents historically has been that the threat actors do not need to actually take the data to be successful, and many times we don't see any indication that data was removed from the victim network. Disclosure obligations can be quite costly, and ransomware attacks have typically not needed disclosure workstreams. Our scope determination is based on an investigation of the available forensic evidence. Companies working with legal counsel can often reach a defendable conclusion that no breach disclosures must be made. The specter of exfiltration in connection with ransomware ups the stakes considerably: should the trend continue, it may mean notification will become a standard requirement on every ransomware event, adding to the response costs and litigation risk to the victim companies.



Ransomware: Vertical Sectors

No industry is immune from the threat of ransomware; Crypsis responds to attacks on organizations of every shape and size. The discussion further in the report focuses on specific industries with unique ransomware risks and challenges. The goal of ransomware is total business disruption, making victims choose between paying the ransom or rebuilding their affected systems, often from the ground up. For critical industries like healthcare and government, disruption is often not an option for the constituents or customers they serve. For financial services, legal, or manufacturing organizations, the disruption leading to downtime may cost the companies millions for every day they are offline.

Healthcare

The Health Insurance Portability and Accountability Act (HIPAA) and the protections it provides to U.S. patients has prioritized the safety of sensitive medical information. As a result, the cost of sensitive data exposure has gone up dramatically for those in the Healthcare sector. Additionally, healthcare providers serve critical functions to people in need; emergency rooms, operating rooms, and supporting healthcare ecosystem providers do not have the luxury of downtime, making the Healthcare sector a prime target for ransomware threat actors. The prevalence of interconnected, high availability medical devices makes security a challenging priority for healthcare organizations, something threat actors are quick to exploit.

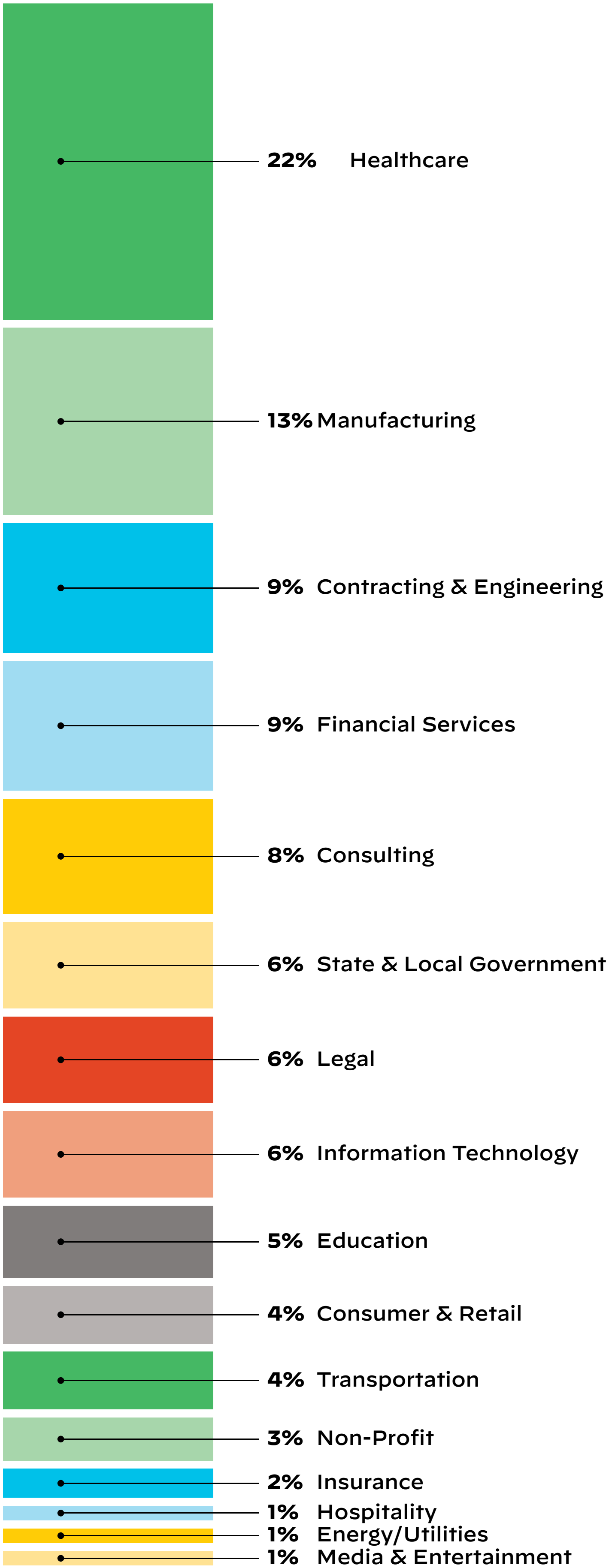


Figure 6: Ransomware cases by vertical sector, 2019

Manufacturing

In 2019, Crypsis observed a 73% increase in ransomware attacks on manufacturing operations over 2018. Ransomware attacks in a factory setting can cripple a business's ability to produce product, leading to days if not weeks of down-time to their significant financial detriment. Ryuk ransomware has been used as the malware of choice in 50% of our Manufacturing sector cases.

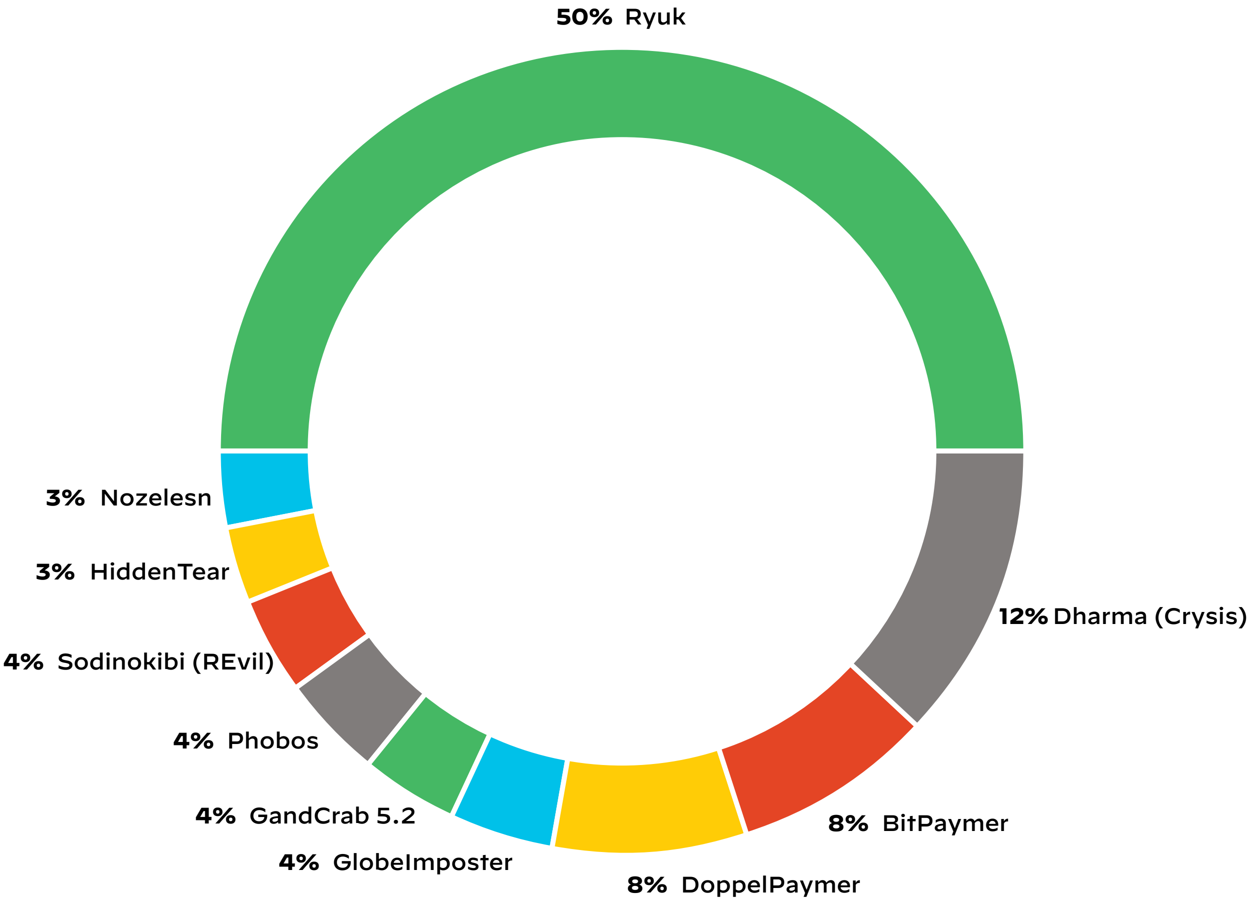


Figure 7: Most common ransomware variants (percentage of incidents) seen in manufacturing matters, 2019

Information Technology

Information technology providers, specifically Managed Service Providers (MSPs), are closely interconnected with their clients. For small businesses or organizations without dedicated internal IT and security personnel, this can offer significant cost, scale, and expertise advantages. However, when a threat actor compromises an MSP's network, it often puts all their clients immediately at risk. In 2019, threat actors were able to use MSPs as an entry point to countless victims during a ransomware attack. Crypsis observed a 185% increase in attacks against information technology providers over the past year.

Financial Services

Across the globe, those in the financial industry act as the gatekeepers to huge amounts of sensitive financial data. The integrity and safety of that information is critical for these firms' business operations and their reputations. A ransomware attack against a financial firm not only puts large amounts of financial information at risk, but also cripples the firm's ability to conduct financial transactions, potentially putting millions of customer dollars and contracts in jeopardy.

> Ransomware monetary demand amounts are trending up; threat actors have evolved, are employing more sophisticated tactics, and are adding data exfiltration and extortion to the mix.

Attacks on State and Local Government

In 2018 and 2019, Crypsis observed nearly 50 ransomware attacks on city and state government services, spanning 17 different states. State and local governments present a unique challenge: Municipalities are a prize for threat actors because they generally have a stream of revenue with which they can pay a ransom, manage critical systems that would be greatly affected by a ransomware attack (e.g., water, electricity, tax, and financial services), and, in many cases, have legacy systems that are more susceptible to attacks. While they are impacted by the same threat vectors as most other organizations, the lack of Active Directory or network segmentation within many municipalities means that cybercriminals can move laterally throughout the network, providing threat actors access to sow devastation across multiple government organizations and countless devices at once.

The decision of whether to pay a ransom is a challenging financial and risk-based decision regardless of the industry. However, for those who answer to the U.S. taxpayer, that issue can become even more convoluted. Many state or local governments choose not to pay the threat actor's ransom out of principle, opting to restore systems regardless of cost.

ACT**NOW**

RANSOMWARE PREVENTION PRO TIPS

- Regularly create and test backups; ensure the backups are stored off network and are protected so threat actors cannot gain access and disable or delete backups to prevent recovery.
- Adopt account administration best practices across the organization, including requiring unique and complex passwords that are at least 15 characters in length so they cannot be easily brute forced.
- Integrate multi-factor authentication (MFA) for all remote access, internet-accessible, and business email accounts to greatly reduce the organization's attack surface.
- Limit the use of privileged accounts, and do not reuse local administrator account passwords to prevent initial access by attackers, privilege escalation, and lateral movement across the network.
- Move away from flat networks: segregate networks and Active Directories, segmenting sensitive data, and leverage secure virtual local area networks (VLANs).
- Leverage log aggregation systems, such as a Security Information and Event Management (SIEM) system, to increase log retention, integrity, and availability.
- Understand where sensitive data lives and implement strong access controls to protect that data; monitor and audit access regularly.
- Have an Incident Response and Remediation Plan (IRRP): incidents may occur despite best efforts, so have a tested, comprehensive IRRP to ensure fast action should an incident occur. If you have cyber insurance (recommended), be sure to integrate the policy's key processes and contacts into the IRRP.

To prevent vulnerability exploitation:

- Disable any direct external RDP access:
  - Ensure all external remote administration is conducted through an enterprise-grade MFA VPN.
- Upgrade from Server Message Block Version 1 to limit adversaries from using the inherent file sharing protocol to move laterally within the systems.
- Patch all systems as quickly as possible.

Remove systems that are running on operating systems that are no longer supported.

To prevent phishing and social engineering: User education

- The key to successful employee training is creating curricula tailored to the organization and employee roles and that take into account the fast-evolving nature of threat actor methodologies:
  - Create a "security awareness culture." It is essential that company leaders buy into the importance of cybersecurity, support and promote richer cyber training programs, and emphasize security in company communications.

Continued on next page >

RANSOMWARE PREVENTION PRO TIPS *(continued)*

- Tailor web-based modules customized to individual groups pertinent to their roles and how they may be specifically targeted so employees can better spot and avoid tactics that may be used against them.
- Make phishing tests incrementally harder to track your organization's strengths and weaknesses, so you can then custom-build phish testing focused on areas of weakness.
- Develop comprehensive training that includes, and goes beyond, phishing and spear phishing; include other social engineering concerns that involve physical security, industry best practices against device loss, insider threat indicators, etc.
- Gamify security training to better engage employees by setting goals, rules for reaching the goals, rewards or incentives, feedback mechanisms, and leaderboards (organizations can compete against each other).
- Hold across-the-board training annually and a mid-year "refresh" that builds on specific areas of emphasis, such as advanced techniques for all employees.

BUSINESS EMAIL COMPROMISE

BEC—the unauthorized access to an organization's email system in an attempt to commit fraud or data exfiltration—continues to be one of the most prevalent attack types organizations face. It represents 34% of the incidents we investigated in 2019, a reflection of its popularity with threat actors. While no doubt convenient for IT administrators, organizations' migration from on-premise email servers to cloud-based email solutions like Microsoft Office 365 and Google G Suite over the past few years has been a boon for threat actors. Never before have more organizations had email accounts directly accessible from the internet. And without MFA in place, stolen credentials often lead to a compromise with full access by the attackers.

While Crypsis sees countless spam and untargeted BEC attempts, we have also witnessed a rise in targeted attacks and the sophistication of methods used against organizations over the past two years.

TOP THREE PRO TIPS TO PREVENT BEC ATTACKS

1

Employ regular and robust security awareness training to combat phishing attempts.

2

Implement MFA as a security policy for all employees.

3

Require that wire transfer verification takes place outside of email to ensure a multi-step verification process.

Read a detailed list of BEC prevention pro tips on page 28.

Recently, we have observed increasing evidence of pre-attack reconnaissance. To initiate a targeted attack, threat actors appear to be identifying and researching victim organizations to understand the industry and the likelihood of success of their fraud campaigns. Once their external research is complete, attackers commonly leverage spear phishing emails in an attempt to steal credentials, targeting executives or those with high-level credentials and financial or sensitive data access, such as the CEO, accounting team, or finance department. When the spear phishing attack is successful, the threat actor has gained privileged access and an inside view to learn how the victim company's wire transfer process works, how the owner of the compromised account writes, and how they communicate with others in their organization. Threat actors then set up the infrastructure they need to be successful, such as creating fraudulent domains that mimic the organization's. Crypsis has seen threat actors closely replicate the legitimate payment process used by organizations, such as by copying spoofed email addresses and creating fake purchase orders for parties expected to be on such communications.

Once the attack is complete, a common threat actor tactic is to use the initial victim's account to initiate malicious spam or jump to additional accounts they may have discovered in the initial attack. Data may be exposed if it is stored in the victim's email account, including sensitive personally identifiable information (PII) or electronic protected health information (ePHI).

BEC and Sensitive Data Exposures

While stealing data is not the primary objective in BEC cases in our experience, it occurs, and data can be exposed, resulting in reputational damage, litigation risk, and other adverse outcomes. In 2019, 48% of Crypsis's BEC cases resulted in the determination of a breach of sensitive information requiring data discovery, exposing over 9,400 individuals' records on average per incident. In 90% of these cases, the data exposed included names and dates of birth. Over 80% of incidents included Social Security numbers, tax IDs, financial records, and medical records that were exposed during the attack.

> In 2019, 48% of Crypsis's BEC cases resulted in the determination of a breach of sensitive information.

Threat Actor Intent

The most common motive in BEC attacks is financial fraud. Attackers target organizations that move large amounts of money in an attempt to receive a five- to six-figure pay out, causing major disruption to procurement, accounts payable, and supply chains. In 2019, BEC threat actors stole an average of $264,117 from victims per incident; we have witnessed BEC actors steal as much as $5M in a single incident over the course of the past several years.

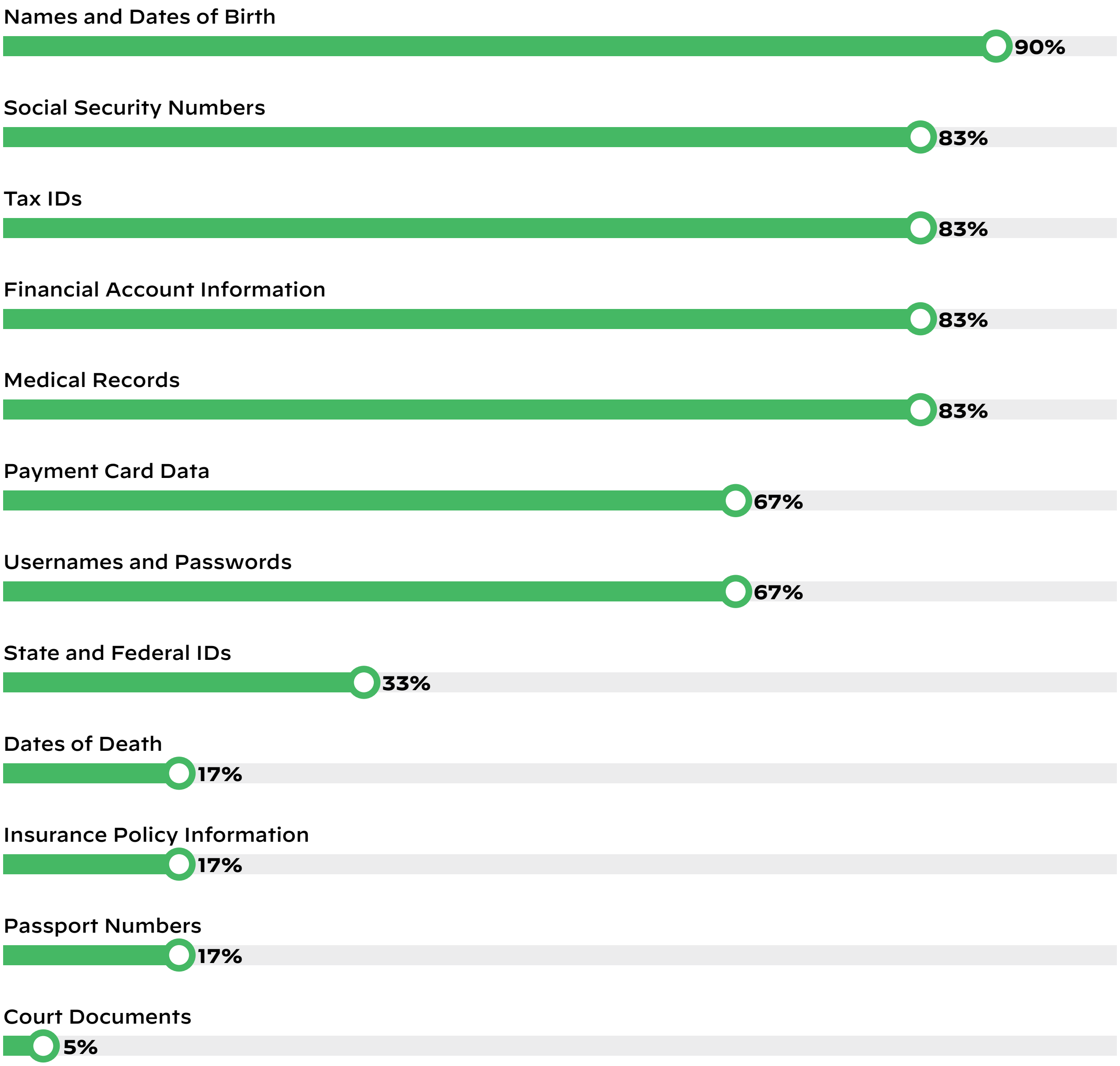


Figure 8: Most commonly exposed sensitive data types in BEC cases

BEC: Vertical Sectors

Regardless of industry, organizations’ access to email to communicate sensitive information and facilitate payments can be disrupted when a breach occurs. Industries, especially those with large volumes of financial transactions, can be particularly appealing to threat actors.

Financial Services

Because of the large volume of financial transactions financial services organizations handle every day, they are the number one target in our 2019 BEC cases, comprising almost 18% of the total. From banks to local real estate firms, threat actors target these organizations because of the access their employees have to large sums of money. For organizations like title companies, the risk goes beyond the firm and can affect customers who are preparing to wire large payments to purchase houses, for example.

Healthcare

In 2019, attacks against healthcare organizations accounted for 15% of all Crypsis BEC investigations. Like the vast majority of BEC attacks, threat actors here are motivated by financial fraud. The opportunity to exploit the invoice process makes healthcare organizations an appealing target for threat actors. Healthcare organizations frequently send and receive invoices for expensive medical services, solutions, and technology. If cybercriminals can insert themselves into this invoice process, they could potentially steal significant monetary assets from organizations and patients alike.

Consulting

Consulting practices rely on senior consultants to regularly bill clients, and, often, many employees are authorized to send and respond to billing invoices in the consultant-client relationship via email. Thus, there is ample opportunity for a threat actor to place him or herself in the middle of the exchange. If the client does not have a multi-step financial verification process, the threat actor could manipulate them into sending the payment to a malicious account.

Manufacturing

Manufacturing companies are also targeted by BEC attackers, as they often send and receive a large volume of payments via electronic invoices. Manufacturing companies regularly purchase supplies or sell to customers in large quantities, leading to a high number of large-dollar invoices.

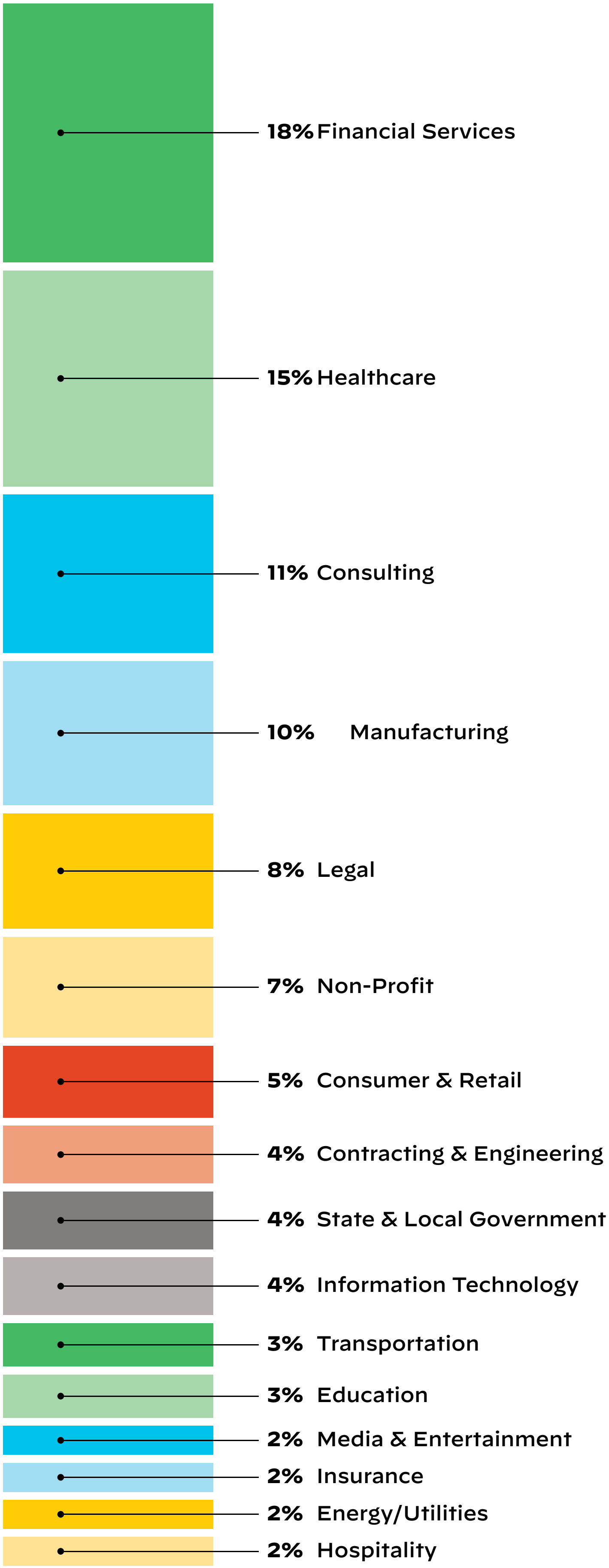


Figure 9: BEC cases by vertical sector, 2019

ACT**NOW**

BEC PREVENTION PRO TIPS

- As the majority of BEC cases are a result of a successful phishing attack, employee vigilance is paramount. See the To prevent phishing and social engineering: User Education section on page 21 for Pro Tips on building a strong employee security awareness culture at your organization.

- Include training on how to identify and manage fraudulent financial requests, even if the request appears to be coming from a valid email address of a colleague—or even a superior.

- To help prevent unauthorized access of email accounts through credential-stealing phishing campaigns, implement MFA as a security policy for all employees.

    - To prevent threat actors from circumventing MFA, disable legacy authentications/protocols and confirm that MFA is not only deployed, but that employees are also using it correctly.

- To mitigate the primary method of BEC fraud, ensure that financial wire transfer verification steps are conducted through non-email communication channels (text messages, voice phone calls, etc.).

- Limit the number of employees authorized to approve wire transfers and provide additional training for authorized employees.

- Use anti-spoofing and email authentication techniques, like Sender Policy Framework (SPF).

- Require unique and complex passwords that are at least 15 characters in length so they cannot be easily brute forced.

- Implement blocking or alerting for auto-forwarding rules that forward messages externally.

- Create custom retention tags for email that: automatically move older items to archive; delete items older than a certain age (e.g., five years); and permanently delete items no longer needed (e.g., those older than seven years) from both primary and archive mailboxes. Keep in mind, however, that archival policies should align with compliance requirements. Consider blocking account logins based on geographic regions if not needed for normal business operations.

- Adopt advanced phishing protection/machine learning solutions like those offered through Microsoft Office 365 Advanced Threat Protection or other third-party solutions to detect and deter sophisticated phishing campaigns.

Importance of Cyber Insurance

As we've emphasized in this report, cyberattacks do not respect the boundaries of industry, organization size, or location. Cyber risks place a costly burden on companies large and small. With the threat landscape becoming more dangerous every day, it is nearly impossible for organizations to mitigate all cyber risks. With that in mind, risk transfer solutions like insurance can play an impactful role in reducing the financial burden an incident can place on its victims.

According to a 2019 NAIC Supplemental Report[4] capturing data from the 2018 calendar year, there are 140 individual insurance companies providing standalone cyber liability insurance products. Furthermore, the number of premiums paid annually, according to the same NAIC report, are estimated to be in excess of $3.5B. Cyber insurers have taken on the role of partner to their customers, connecting policyholders with technical and legal experts to aid in the response to a suspected security incident, and, in some cases, providing guidance in assessing tools and resources to aid in the prevention of an incident. Crypsis has observed clients without cyber policies struggle to not only manage important financial and technical decisions in the middle of a cyber incident, but also prepare for the possibility that they may never be able to fully recover from an attack. It is our position that cyber insurance is a vital tool in transferring the financial burden a cyber incident may place on any company operating in this increasingly digital world.

> It is our position that cyber insurance is a vital tool in transferring the financial burden a cyber incident may place on any company operating in this increasingly digital world.

[4] Denise Matthews, *Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement,* National Association of Insurance Commissioners, (Sept. 12, 2019), https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf.

DATA BREACHES

Aside from ransomware and BEC threats, which merit focused attention, our data breach incident response investigations can be grouped into three main categories: network intrusions, inadvertent disclosures of sensitive data, and insider threats. Taken together, these threats comprise the most impactful—and in some cases, overlooked—areas of risk to the enterprise security armor. They often lead to the large-volume breaches that affect millions of individuals globally. Let's explore the tactics threat actors use to be so successful in these attacks and what organizations can do to build their defenses.

Network Intrusions

Web Application Compromise

Web application attacks are frequently used by threat actors to gain unauthorized access to networks: these applications are commonly public facing, and attackers can spend days or months trying various exploit methods. However, they only have to be successful with one. JavaScript is a popular tool for creating dynamic, interactive web content; yet, developers often leverage reusable packages, which can contain security vulnerabilities. In web development, there is a world of open-source code, but not a lot of time for developers to understand every line of code.

Technical staff are also finding new solutions to store and manage data at scale, and these solutions frequently must interact with each other—but misconfiguration can occur that allows unintended exposure to the public.

Gaps in operating systems or application patching can be a significant root cause of web application attacks. Vulnerability and patch management are well-communicated best practices throughout the industry; but it can be both challenging to keep up with patching cycles as well as disruptive to business operations. Organizations of all sizes can struggle with implementing a solid, end-to-end process for identifying vulnerabilities, prioritizing needed fixes, testing patches, and applying them across geographically dispersed sites. Patching can consume a large portion of staff time if done properly. For large enterprises, the scale of the challenge can be difficult to overstate; for SMBs, staffing challenges can lead to patching gaps and gaffes. Legacy systems and compatibility issues with existing applications/operating systems complicate the process further. When vulnerabilities, new patches, and proof-of-concept (POC) hacks are announced, the race is on to patch systems before hackers can exploit the vulnerabilities. Too frequently, organizations fall behind, and breaches occur.

Web application compromises can also yield our next category of network intrusion: payment card breaches.

TOP THREE PRO TIPS TO PREVENT NETWORK INTRUSIONS

1

Employ Endpoint Detection and Response: be ready to detect issues arising within your network assets and act should an issue occur.

2

Use solid web development practices, but also test them: conduct regular code and site reviews and patch regularly.

3

Conduct periodical penetration testing to determine if you have gaps in applications, software, network defenses, employee awareness, etc.

Read a detailed list of network intrusion prevention pro tips on page 34.

Payment Card Breaches

Several years ago, retail data was most often compromised at the point of sale (POS) using hardware-based card "skimming" or "scraping" devices designed to capture card data. With the adoption of Europay, Mastercard, and Visa (EMV, aka chip and PIN) technology, card-present fraud has largely given way to an increasing prevalence of web-application-based payment card breaches, using malicious software-based card scraping code on POS operating systems or the checkout page of an e-commerce website. Payment card data is highly monetizable and is often both stolen and then sold in bulk, and there can be long lead times from malware injection to discovery.

In 2019, our data set revealed that the **Consumer & Retail and Information Technology sectors fell victim to the majority of payment card breaches,** though other types of industries processing card data online were victimized as well. Consumer & Retail has traditionally been an obvious top target for breach attacks; however, an ever-increasing number of web-based services are offered today, accelerating threat actors' opportunities to victimize organizations and their payment processing flows.

Malicious JavaScripts, software-based card scraping malware, and, in one case, credential-harvesting phishing attacks that led to "Super User" account access/control were the primary methods used to steal card information.

CASE STUDY

Online Gift Shop Suffers Shopping Cart Injection

A non-profit organization learned that it had malicious code, which was designed to steal payment card information, injected into its online gift store payment processor gateway. After believing it removed the code, it engaged The Crypsis Group to learn how the "shopping cart injection" code found its way onto its site. However, while scoping the engagement, the Crypsis experts discovered that the code was still there: the source of the code had not been addressed, and it had automatically reinstalled into the shopping cart processing page. After a complete review, the Crypsis team discovered that the threat actors had installed malicious code into the back-end database, which had then inserted a footer on every page of the website. The organization had directly removed the line of code on the shopping cart page; however, the back-end database automatically scanned the site, discovered the footer missing, and reinstalled it, and with it, the data-stealing functionality. After being told by its third-party development team that the only remedy would be to take the store offline for several days while remediation ensued, Crypsis had a much more streamlined solution for the organization: they pointed the organization's technical team to a single line of code in the back-end database that should be deleted, eliminating the problem.

Advanced Persistent Threat (APT) Nation State Attacks

While many of the attacks in this report have clearly defined, short-term motives of monetizing the illicit access, APT attacks are typically more stealthy, designed to remain undetected for long periods, and the specific motives less clear. APT attacks require a high degree of expertise and resources and are typically waged by well-funded nation state threat actors. They often target organizations with desirable intellectual property or trade secrets, or government entities, utilities, and other types of critical infrastructure. APT attacks can be initiated with social engineering or spear phishing attacks, but may also use advanced zero-day exploits. From the initial attack vector, the APT actor works to gain further access, maintain persistence, set up backdoors, and ensure they can exfiltrate data unnoticed by the organization for extended periods of time. They may go to extreme lengths to evade detection, including disabling detective controls, clearing logs, remaining dormant for long periods of time, or periodically deploying new malware. Other APT attacks target large volumes of sensitive PII, such as personnel records or credit files, presumably for use in large-scale intelligence-gathering operations.

CASE STUDY

Crypsis vs. APT41: Tech Company Suffers APT Attack

Early last year, an innovative technology company was notified by the FBI that it had reason to believe that data had been exfiltrated from the company's network. The company turned to The Crypsis Group to investigate and determine if unauthorized access had occurred, the scope of this access, and the extent of data exfiltration. Crypsis experts concluded that the company had been hit by a nation state-sponsored group, known to some as APT41. The APT41 group, commonly attributed to Chinese nation state actors, frequently targets technology companies, as well as telecommunications, healthcare, and other sectors rich with intellectual property. Crypsis found that APT41 executed an encoded PowerShell command against a vulnerable Confluence server that dropped a JavaScript-based web shell to provide interactive access. We discovered four additional web shell backdoors on the server. The APT41 actors harvested credentials with Mimikatz and pivoted to a JIRA server, placing a web shell onto it, and began staging malware in the root of the recycle bin and "C:\Windows\Temp" directories for further exploitation and reconnaissance. They also pivoted to a domain controller and leveraged the "C:\Windows\Temp" folder for staging, execution of binaries and files of unknown intent, and created a user account. The threat actor utilized the archiving utility WinRAR to compress and encrypt data in 1 GB chunks and stage it for exfiltration within a maliciously created subfolder of the recycle bin directory, on a non-operating-system partition. Crypsis found that they were exfiltrating software code, which is a common target of APT41 actors. Crypsis was able to validate this company's concerns, support its cooperation with federal law enforcement, and advise it on steps to avoid this and other APT actors' future attempts.

ACT**NOW**

NETWORK INTRUSION PREVENTION PRO TIPS

Web Application Compromise

- Follow a defense-in-depth approach, implementing safeguards at each layer of the web application stack. While the list can be long, it can include (for example) web application firewalls, operating system hardening, application input controls (e.g., parameterization, validation), file integrity monitoring, least-privileged user accounts for database access, and industry-standard encryption.

- When implementing open-source code, research it to understand if it has any published vulnerabilities; only use code that is vetted and patched.

- Collect, retain, and regularly monitor logs.

- Conduct regular web application/code reviews and consider periodic penetration testing to search for vulnerabilities; follow remediation recommendations.

- To help avoid breaches due to patching gaps, establish and strictly adhere to a patching management process to patch all applications and operating systems. At a minimum, consider these Pro Tips:

  - Inventory all IT assets (including storage, switches, laptops, etc.) across the entire distributed organization through automated discovery tools to get a clear picture of what you have to manage.

  - Prioritize your patching needs: determine which represent high, medium, or low risk, and their level of priority for the business.

  - Supplement that list by researching vulnerabilities for all operating systems, applications, etc., and add those to your list of priorities to address every month.

  - Any vulnerabilities that have published POC code should be considered in the "high" risk category to fix.

  - Test your patches in a development QA environment to ensure they won't "break the system" once deployed into production.

  - Have a schedule for deploying patches regularly: for some companies, that may only be once a month; however, ensure you are able to deploy high-priority patches out of cycle when necessary (such as those for which POCs have been published).

  - Once patches are deployed, monitor them for stability.

Payment Card Breaches

- To help protect customers and defend against payment card breaches, organizations that store, process, or transmit payment cards should adhere to the PCI Data Security Standard5 (PCI DSS) as a baseline.

  - The standard is designed to identify/assess all locations and assets that process or store card data, analyze them for vulnerabilities, repair gaps, and then document the process via compliance reports.

Continued on next page >

- Because many card breaches begin with web application compromise, we recommend paying particular attention to the web application compromise Pro Tips above, with the following nuances for card scraping tactics:

  - Deploy Web Application Firewall (WAF) technologies: behavioral-based utilities that monitor attempts to insert code. They are effective at spotting shopping cart injection techniques.
  - Limit "write" permissions on the web server to only those that require them.
  - Restrict permissions to your web server account.

APT Nation State Attacks

- Leverage Endpoint Detection and Response solutions to have full visibility to activity across all endpoints and respond faster. Patch management is critical for operating systems and on-premise applications: APT actors will move very quickly to capitalize on vulnerabilities. Address new published vulnerabilities immediately.
- Identify your organization's critical and most valuable assets. This should include conducting an inventory of critical assets to understand where your highest-value targets are and if they require any additional protection.
- Regularly review Active Directory for newly created accounts, mailboxes, and group policy objects.
- Implement a log retention repository and regularly review all logs and login attempts for any unusual behavioral patterns. This will allow you to monitor the activity of an APT if a breach occurs.
- Conduct regular security awareness training. See the To prevent phishing and social engineering: User Education section on page 21.

[5] Payment Card Industry (PCI) Data Security Standard, PCI Security Standards Council, (June, 2018), https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-AOC-Merchant.pdf.

Inadvertent Disclosure

While ransomware tends to grab more headlines, threat actors capitalizing on inadvertent disclosure (the accidental exposure of sensitive data) often results in more breaches and exposes more sensitive data than other types of security incidents. One recent study[6] indicated that 2019 was the worst year ever for data breaches—and threat actors taking advantage of inadvertent disclosure incidents involving cloud implementations were the primary culprits. In 2019, Crypsis led ~80 inadvertent disclosure incident response investigations, and, if our current rate holds, is on track to double that rate in 2020—perhaps owing to an increasing use of cloud solutions as organizations work to leverage the efficiencies, cost advantages, and scale they offer.

For our purposes, "inadvertent disclosure" comprises any type of security incident that results solely from non-malicious actions by an individual with authorized access to the sensitive data; these actions created a situation in which the data could be made available to unauthorized individuals. Additionally, the data may or may not have been actually accessed or stolen. Threat actors are continuously scanning the internet for data exposed in this manner, and such low-hanging fruit makes for easy monetary gains. Some automated internet indexing utilities will also find exposed data, presenting it to the masses.

In 2019, 45% of Crypsis's inadvertent disclosure investigations resulted in a data breach determination. These matters required us to employ data discovery processes to determine which types of sensitive data were exposed so legal teams could make determinations on whether breach notifications must be made to affected parties as set forth by various industry, state, or regional guidelines. The clients requiring data discovery belonged to the Healthcare, Information Technology, Financial Services, and other sectors; thus, significant volumes of ePHI, PII, and other data types were exposed from inadvertent disclosure events in our 2019 sample.

TOP THREE PRO TIPS TO PREVENT INADVERTENT DISCLOSURE

1

Audit your data assets: know where your sensitive data resides and who has access to it throughout the organization and in your third-party supply chain.

2

Limit access to only those who need it in your organization and with third parties.

3

Ensure technical staff and employees are trained on security risks pertinent to their roles in the company.

Read a detailed list of inadvertent disclosure prevention pro tips on page 41.

[6] Jai Vijayan, Third-Party Breaches — and the Number of Records Exposed — Increased Sharply in 2019, Dark Reading, (Feb. 12, 2020), https://www.darkreading.com/attacks-breaches/third-party-breaches---and-thenumber-of-records-exposed---increased-sharply-in-2019/d/d-id/1337037.

While BEC incidents led to an even higher breach determination rate (48%), inadvertent disclosure incidents can have a greater impact because they often expose massive data stores (such as those found in cloud databases), as we have seen in numerous breach announcements in the media over the past year. To illustrate, our 2019 inadvertent disclosure cases exposed 713,000 individuals' records, on average (conservatively estimated); our 2019 BEC matters only exposed an average of 9,400 individuals' records. (In BEC, the primary objective is most often wire fraud, and data exposure is a collateral outcome; read more about these cases in the Business Email Compromise section on page 23.)

The data lost in these events can span from intellectual property to ePHI, Social Security numbers, passport numbers, payment card data, corporate emails that can be used for blackmail, and more.

For our purposes, inadvertent disclosure events include:

- **Exposed cloud data,** resulting from flaws in cloud implementation
- **Misconfigurations** that result in improper security posture of a system
- **The physical loss of electronic media,** e.g., via the loss of a laptop, external hard drive, or hand-held device

Top Cause of Inadvertent Disclosure Events in 2019

Cloud Exposures

In 2019, the majority of the inadvertent disclosure incidents we investigated were cloud exposures. This is hardly surprising: the cloud has become the dominant, enabling computing paradigm that companies of all sizes are embracing; yet, many are struggling with managing multi-cloud and hybrid cloud woes. Let's explore why the cloud creates such significant security challenges for organizations.

> 45% of Inadvertent Disclosure Events Resulted in a Breach Determination in 2019, Exposing 713K Individuals' Records per Incident on Average.

The Cloud Conundrum

While companies increasingly seek to leverage the enabling advantages of cloud solutions, there remain significant complexities that enterprises must address to protect their cloud data assets. For each CSP, there is an almost dizzying array of tools, capabilities, and user-driven security settings designed to secure them, extending far beyond the S3 bucket issues so commonly referenced. Each cloud provider's tool sets and security best practices differ; and, given the plethora of capabilities and controls within each platform, multiplied by the ever-expanding number of proprietary platforms leveraged by the typical organization in a multi-cloud world, it's no wonder cloud security has become a vexing issue, stretching the capabilities of even senior security staff. And staff must command a high level of expertise, as the degree of complexity leaves many opportunities for error. Cloud providers are doing more every year to help users avoid errors (for example, Amazon Web Services [AWS] has recently introduced a setting at the bucket level or account level that disables the ability to set S3 data to "public"—a helpful move for service users). Yet, the issues remain: SMBs typically lack the expertise to manage the complexity, and large enterprises can face challenges due to their very high usage of multiple cloud platforms across a diverse, dispersed IT landscape—especially considering that the cloud is only one aspect of the security estate they need to patrol.

CASE STUDY

Popular Social Media Site

A popular online social media site had reason to believe it had exposed a significant amount of consumer data through an accidentally exposed, third-party-hosted database. The Crypsis Group forensic experts validated its concerns: anyone who found its exposed port could query the data, which contained PII. The port was exposed following a database configuration change. Confounding the investigation, the database was configured to only log errors—not successful queries. There were no firewalls, load balancers, or other network infrastructure in place that could have determined whether the data was accessed.

Crypsis used DataDog, a third-party utility used to track server metrics, to determine that network usage remained consistent during the window of exposure. DataDog tracks processor usage, memory usage, disk errors, and daily network bandwidth (bytes transmitted and received). Logs are retained, at least for this client, for over a year. Not only did that cover the window of exposure, it gave the team a baseline of what "normal" looks like for six months prior to the exposure. DataDog only showed a large "spike" at the end, representing Crypsis's queries into the database as we were identifying the data it contained. (It is not uncommon for an attacker to do this type of identification when they gain access to a database, but no other spike was seen.) Crypsis was able to validate this finding using the atop utility included in many Linux distributions. Atop monitors processes from the time they are started and tracks metrics such as disk I/O and network utilization. Atop showed high levels of disk "write" activity for Java, but low levels of "read" activity, as well as a consistent network utilization seen in DataDog. Together, these findings helped the client and its legal counsel draw conclusions regarding its data breach notification obligations.

Misconfiguration

"Misconfiguration" errors—improperly establishing (or failure to establish) security settings in systems—can affect any layer of the application stack, from operating systems, to web and application servers, firewalls, and applications. Misconfiguration is included in Open Web Application Security Project's (OWASP's) Top 10 list of most critical application security risks. Penetration tests often identify misconfiguration errors across the IT infrastructure, but where applications are internet-accessible, threat actors often find those same vulnerabilities before the white hats do.

Common examples of misconfiguration errors include: neglecting to change default account passwords on applications and servers; deploying development configurations into production (leaving tracing elements threat actors can follow to insecure accounts); leaving more open ports in firewalls than necessary or allowing unauthorized hosts to connect to the server; leaving "debugging" or "setup/configuration" pages enabled; enabling directory listings; failure to secure directories; and a host of other common pitfalls.

Inadvertent Disclosure: Vertical Sectors

Inadvertent disclosure incidents span all vertical sectors. However, because many of these errors are the result of digital transformation and the use of cloud technologies, we see patterns emerge: Our top vertical sectors affected by inadvertent disclosure events in 2019 were in the Information Technology, Financial Services, and Healthcare sectors.

Information Technology

Information Technology, in our client set, includes e-commerce platforms, online collaboration and services platforms, CSPs, and innovative technology development companies. A majority of these organizations maintain significant data stores. Because they are technology heavy, we see them at the top of the heap in our inadvertent disclosure cases, representing 18% of these incidents in 2019.

Financial Services

While "Financial Services" often summons images of large, global banks, it's important to remember this sector includes credit unions, accounting firms, real estate agencies, and financial advisories, as well as banks and lending institutions. These come in many sizes, and, often, smaller firms don't have expert staff to manage cloud implementations, or other IT functions that would help avoid inadvertent disclosure issues. Their data, however, is highly monetizable, and when they spring a leak, attackers are quick to capitalize on it.

Consulting

Increasingly, healthcare organizations, many of which are strapped for cash and lean on skilled IT staff, are leveraging cloud solutions for everything from billing to health monitoring, remote patient care options, online patient portals, and more. Yet, offloading work to the cloud doesn't offload all of the security burden, and healthcare delivery organizations, as well as associated technology providers that leverage technology platforms, have seen a number of related inadvertent disclosure events, often exposing volumes of sensitive data.

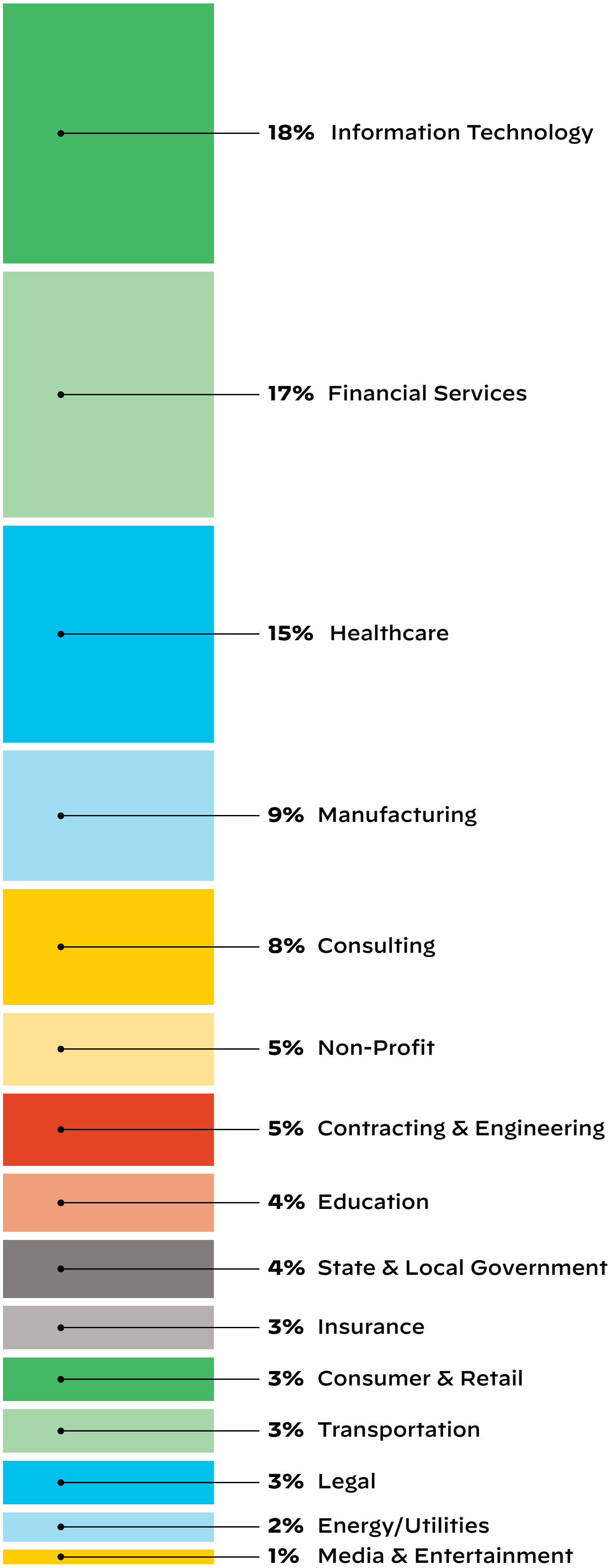


Figure 10: Inadvertent disclosure cases by vertical sector, 2019

Sensitive Data Exposure

We can see the high incidence of breaches in the Financial Services and Healthcare sectors reflected in the types of sensitive data exposed throughout 2019. While most sensitive data exposures will include records that reveal names, dates of birth, and often Social Security numbers, we can see financial records, tax identification numbers, and medical records commonly appear in our data findings, showing the frequency with which Financial Services and Healthcare are affected by this security malady. Information Technology sector victims tend to expose a broader span of data types, which can appear across the entire spectrum. Healthcare and Financial Services were the two sectors most likely to experience an incident resulting in a breach determination in 2019.

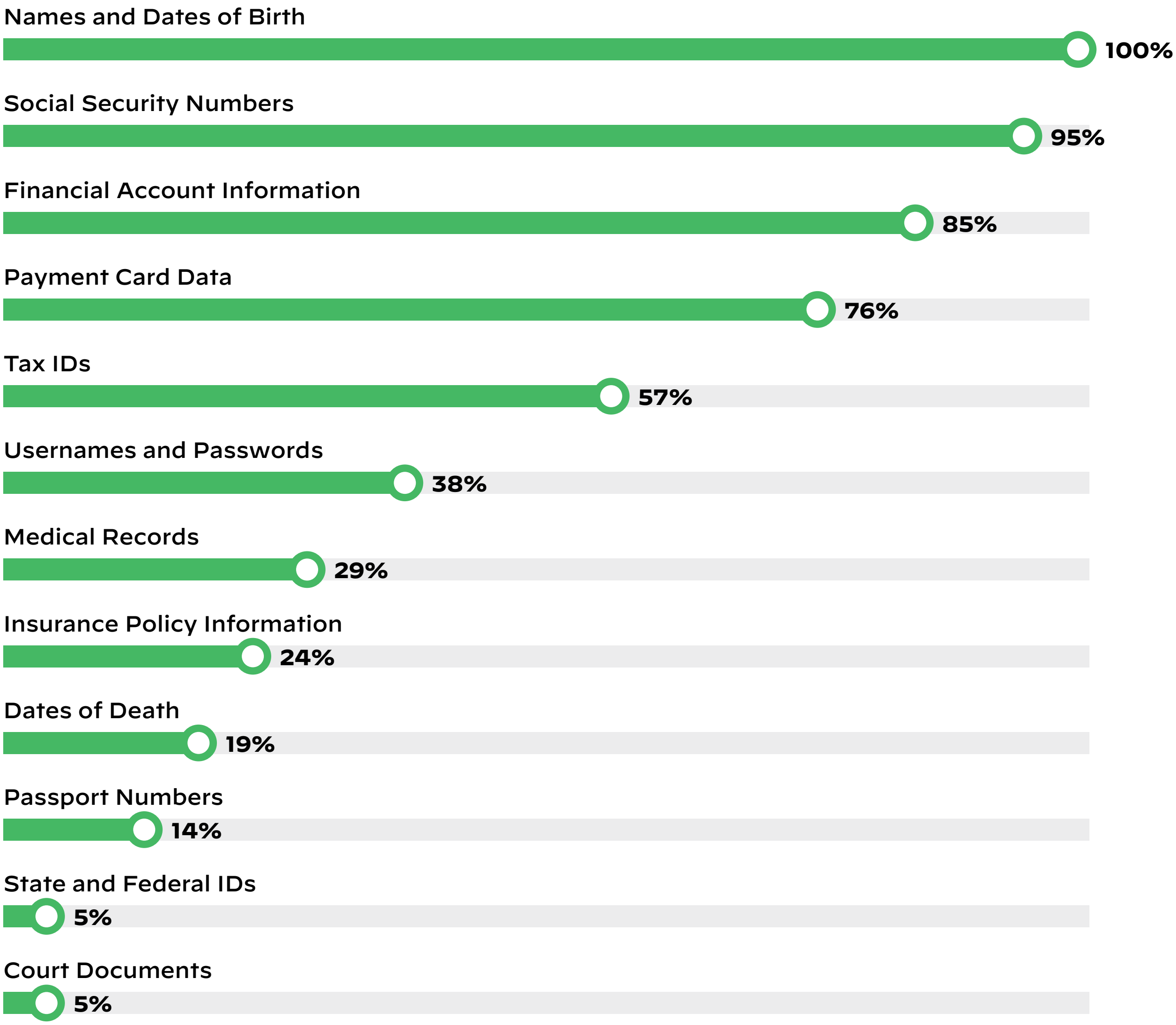


Figure 11: Most commonly exposed sensitive data types in inadvertent disclosure incidents, 2019

ACT**NOW**

INADVERTENT DISCLOSURE PREVENTION PRO TIPS

Exposed Cloud Data

The following Pro Tips are recommended to address cloud-related data breaches:

- **Leverage expertise in cloud security, per platform.** Managing security in the cloud requires expertise, catered to the nuances of each platform. The more complex the platform, the more plentiful the opportunities for errors that can inadvertently disclose data. To help ensure cloud platforms are secure:
  - Ensure users with cloud control access are fully trained in each cloud environment.
  - If you do not have the in-house expertise, or your cloud estate is particularly complex and in a continual state of change, evaluate your options for managed security services. Cloud providers offer managed services to continually monitor cloud security, configurations, and access, but other companies offer them as well.
- **Control access to the cloud environment.** Access to cloud controls, such as CSP consoles, application programming interfaces (APIs), and command-line interfaces in the cloud should be restricted to only those who need it. Such role-based access control (RBAC) is essential to minimizing risks of configuration and other security errors. Additionally:
  - Use MFA for authorized users, as well as certificates and digital signatures.
  - Separate administrative and user credentials and limit everyday users to production environments.
  - Where possible, implement whitelisting to further limit access to known and trusted endpoints.
- **Know what data you have in the cloud and where it is.** Regularly audit your cloud data to know what sensitive data you have and where it's located. AWS Macie is a security service that automatically discovers, classifies, and protects sensitive data in AWS. If this is outside of your budget, S3 buckets have a base-level inventory feature.
- **Encrypt it.** Encrypt sensitive data (at a minimum), segment it, provide access using RBAC, and rotate keys regularly. Evaluate whether maintaining keys with the cloud provider or within your organization is the best option for you, but ensure you have a key security policy that limits key access and exposure to risk.
- **Ensure file-level operations are logged.** It's important to have visibility to all historical access and creation/deletion events. AWS CloudTrail doesn't automatically log these events, and logging must be turned on. We recommend ensuring that either CloudTrail or server access logging (an included feature of AWS S3 services) are activated.

Continued on next page >

INADVERTENT DISCLOSURE PREVENTION PRO TIPS

(continued)

Misconfiguration

- Run periodic scans and/or penetration tests that include configuration checks and perform regular system audits to detect misconfigurations; consider annual penetration testing at a minimum to discover enterprise IT gaps.
- Implement change control protocols that require review and sign-off on configuration changes.
- Disable the use of default accounts and passwords.
- Disable administrative interfaces and debugging.
- Configure servers to prevent unauthorized access and directory listings.
- Enforce strong access controls.
- Set security settings in your development environment to a secure value.
- Keep software up to date.

Physical Loss of Electronic Media

- To limit the risks and damage of physical media loss:
  - Implement full-disk encryption for laptops and removable devices.
  - Have corporate policies on device security and include them in security training. Clearly articulate the importance of not leaving electronic media in vehicles, left unattended for even brief periods of time, and the use of hotel safes. Urge employees with access to critical data to purchase PC locks. Educate on the urgency of immediately notifying IT if media is lost or stolen.
  - Limit access to important data and systems to only those that require it.
  - Require rigorous password protocols and MFA for all devices and accounts.
  - Implement and utilize mobile device management applications that have the capability to locate and/or remotely wipe devices.

Insider Threats

While organizations today are often more focused on external threat actors, insiders can pose very real and insidious threats to an organization, on par with (and potentially greater than) external factors. Insiders are anyone we consider an authorized user of our data: employees, contractors, third-party service providers/vendors, and business partners. Trusted, connected, and with time on their side, insiders with access and knowledge of the intricacies of the business and infrastructure can potentially do significant monetary, brand, or competitive damage.

Companies are becoming increasingly aware of the insider threat. A 2019 Cybersecurity Insiders report[7] found that 70% of organizations said they think insider attacks have become more frequent, with 62% most concerned about malicious insider attacks. Our data validates their beliefs: Our insider threat investigations rose 68% (as a percentage of our total overall investigations) from 2018–2019. For the purposes of this report, "Insider Threats" refer to deliberate, malicious data theft by employees; accidental data incidents by employees are addressed in the "inadvertent disclosure" section of this report.

TOP THREE PRO TIPS TO PREVENT INSIDER ATTACKS

1. Conduct security awareness training for all staff that includes indicators of insider threats and provides employees with anonymous vehicles and protections for reporting issues.
2. Implement security and access control policies to limit sensitive data access to "need to know/access" only.
3. Have an IRRP in place, including plans to preserve data for potential investigations.

Read a detailed list of insider threat prevention pro tips on page 48.

[7] Cybersecurity Insiders, 2019 Insider Threat Report, Nucleus Cyber (Apr. 24, 2020), https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf.

Threat Actor Intent

Through our investigations, we see a range of motives and contributing factors that fuel insider threat cases. In our 2019 insider threat investigations, the motive of the majority of our cases appeared to be associated with gaining professional advantage (stealing data or work products to help accelerate an individual's career at another company). For example, we have seen individuals stealing source code with the apparent intent to aid a competitor's software development project (where the individual was leaving to begin a new career); as well as employees stealing electronic engineering diagrams and digital photographs of whiteboards containing sensitive intellectual property for similar purposes.

Crypsis Insider Threat Investigations Rose 68% from 2018–2019 (as a percentage of our total investigative matters)

The second leading reason for insiders taking malicious actions against employers was retribution or acting out a grudge against the employer—for example, one case included an employee intending to be a "whistleblower" against unfair or discriminatory practices.

As you will see later in this section, Financial Services sector companies are well represented in our insider threat data cases; these businesses, which include banking, accounting, real estate firms, and the like, handle large financial transactions and offer ripe opportunities for insider theft—and financial gain was our third leading motive for malicious insider attack in 2019.

While insider threats don't often result in the exposure of large quantities of sensitive data, some do: 6% of our 2019 cases required data discovery to determine whether data breach disclosure was required.

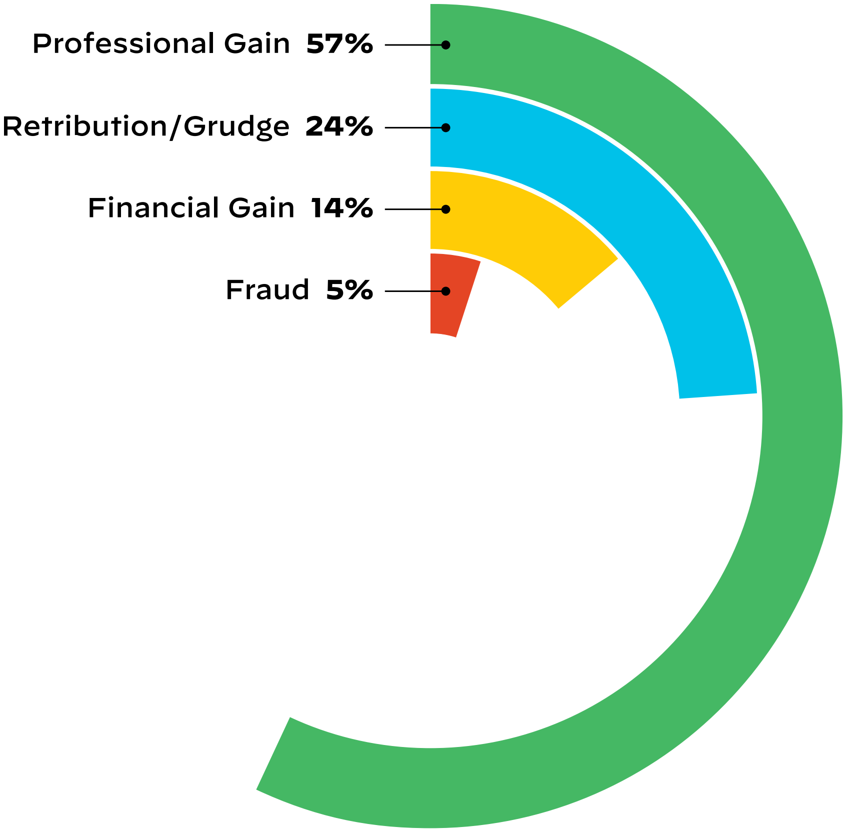


Figure 12: Most common motives for insider attacks in 2019 (where motive identified)

6% of Insider Threat Investigations Resulted in a Sensitive Data Breach

Regardless of motive, timing is key when it comes to monitoring insiders for potential threat activities. Employees planning to leave the business represent the greatest threat to the business and are far more likely to steal data for any number of the motives listed above. The challenge of course is that organizations often don't know that an employee is planning on departing. Controls must be put in place to monitor for aberrant data behaviors (see the Act Now: Insider Threat Prevention Pro Tips section on page 48), and managers can be trained to spot signs of a potentially disgruntled employee. When an employee exits the organization, it is important that companies have a robust exit interview, take custody of any digital media, and employ a rigorous process for ensuring complete, timely access termination.

Attack Methodologies

Insiders use many techniques to attempt to steal data and cover their tracks. Such methods include uploading data to personal cloud storage sites, copying data to USB storage devices, downloading files from company cloud storage mechanisms from home or personal devices, and taking photos/making copies of important documents. To obscure or delete evidence of these activities, insiders often use file wiping/erasing software to destroy evidence and files, clear web browsing histories, and delete or disable Volume Shadow Copies (on Windows systems) to minimize forensic artifacts of their actions. Many will perform their "suspicious activities" after hours or on weekends.

CASE STUDY

Ex-Employee Joining Competitive Firm Steals Then Wipes Data

An employee resigns and joins a competitor working on a similar product. The company suspects the employee shared proprietary information with her new company before resigning; however, the employee returned her laptop a full month later, "wiped" of user data. In this state, what can the company possibly learn about how the computer was used?

The Crypsis Group digital forensics experts ultimately uncovered the theft of intellectual property and destruction of data. We recovered fragments of previously deleted files and other essential forensic artifacts from the ex-employee's laptop. Among the key findings, Crypsis identified evidence that code reviews, rollout plans, and other proprietary information were accessed from thumb drives while the laptop was connected to the network of a competitor (and the ex-employee's new employer) days after she resigned. Most damaging was that digital forensics uncovered the considerable lengths to which she went to mass-delete files and cover her tracks. Just days prior to returning her laptop to her former employer, the ex-employee installed a remote access tool and received an incoming connection from an IP address that resolved to the remote location of an outsourced technician of the company (who was suspected of being a co-conspirator). Seconds after the successful incoming connection, mass deletions occurred on the laptop. Without the use of digital forensics, the company would have never known of the illicit acts performed by their ex-employee (and outsourced technician).

Insider Threats: Vertical Sectors

Crypsis is retained to investigate cases of suspected (and often later confirmed) insider threat activities across every vertical industry. When looking at the range of motives, we can clearly see that some, such as professional gain or retribution, would spare no industry. However, trends appear when we factor in the concentration of skill sets required to be more effective at stealing data, as well as the types of data that would be valuable for sale or gaining competitive advantage.

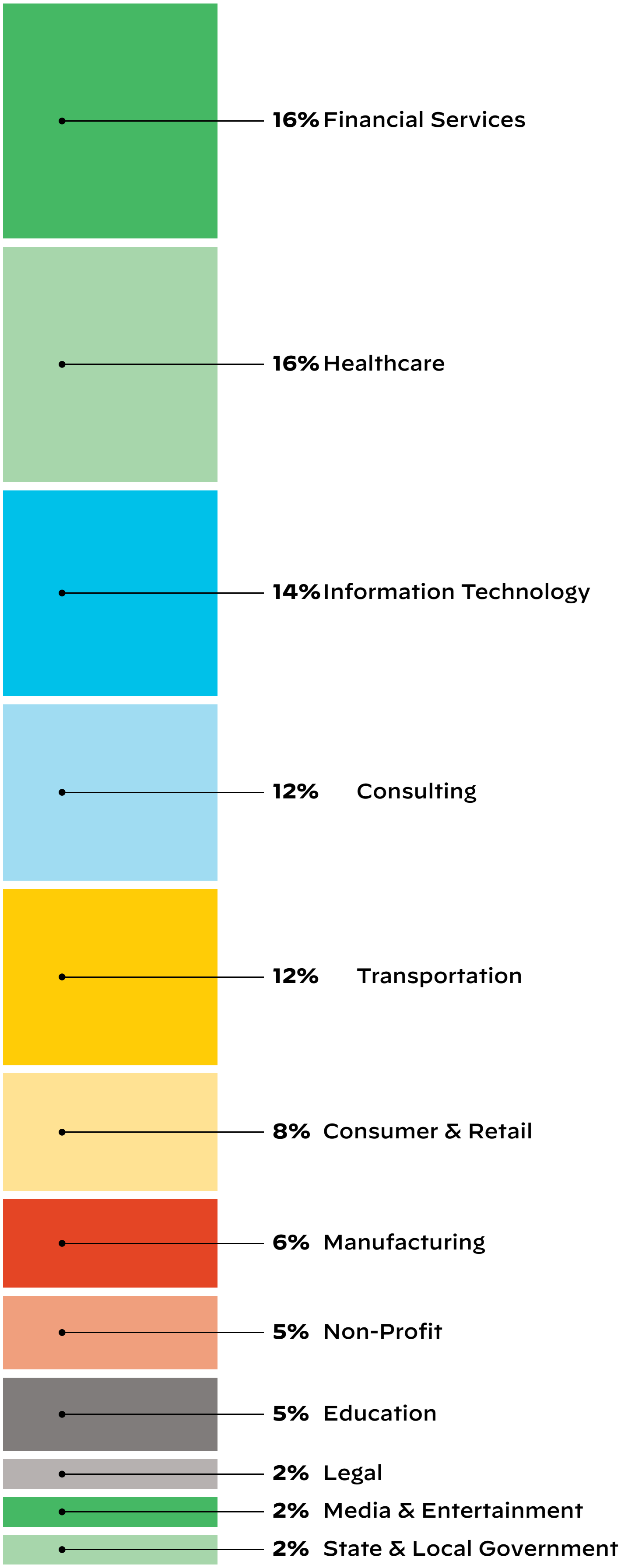


Figure 13: Insider attack cases by vertical sector, 2019

Financial Services

Firms in the Financial Services sector present ripe opportunities for fraud and financially motivated insider crimes, and, together with Healthcare, is the most common vertical sector we assisted in 2019 in this threat type. Financial Services firms gather large amounts of data on their customers—valuable information assets—which are not always properly controlled. This data is valuable to departing employees; can be used to perpetuate fraud; and provides leverage to disgruntled employees looking to harm their employers. For this reason, it's no surprise that this sector is often cited as a top vertical for insider threats. Of note in our data set in 2019: the primary motive in this category was retribution or a grudge against the employer.

Healthcare

Unfortunately, Healthcare once again earns a top spot as an "at risk" sector in our investigations for 2019, this time in insider threats. Like financial services firms, healthcare organizations also collect large and complete data sets on their customers, including full contact information, Social Security numbers, payment card data, and sensitive health information—making it a good opportunity for fraudulent insider acts.

> In our observation, the IT security function within organizations focuses more time and resources on external threats than on internal ones, leaving sensitive data exposed to those who have authorized access and malicious intent.

Information Technology

Information Technology sector companies not only have a high concentration of highly skilled staff with the ability to access data via nefarious means, exfiltrate data, and attempt to delete evidence of their misdeeds, the companies in our insider threat data set included innovative organizations with intellectual property that could present financial rewards or personal career advancement opportunities within a competitive firm. Thus, it isn't surprising that the Information Technology sector earned the number three spot for insider threats.

Consulting

Employees in the Consulting Services sector provide services across a range of industries, offering business process efficiencies and specialized expertise. Their clients' inside information, as well the proprietary methodologies, work product, and deliverables, often constitute highly valuable trade secrets. Too often, Crypsis has seen consulting services company employees misuse this sensitive information for their own personal gain, to trade on inside information, start a competing company, or further future job prospects.

ACT**NOW**

INSIDER THREAT PREVENTION PRO TIPS

While you can't eliminate insider threats completely, it is possible to deter insiders from attempting to misuse their access, detect when they do misuse it, and disrupt further abuse.

Deter

- Develop a strong corporate culture focused on respecting user and company data. Include insider threat indicators into a security awareness training program (e.g., employees coming in after hours or on weekends when they don't really need to, asking questions on topics not relevant to them, etc.).
- Take all appropriate measures to restrict access to only those who need it: consider whitelisting devices and applications. For systems with sensitive information, consider restricting network connections, Bluetooth, airdrop, Secure File Transfer Protocol, USB ports, data transfers, local administrative rights, and internal application permissions.
- Importantly, give your employees a way to conduct their business legitimately—simply blocking certain vectors will result in creative workarounds that you'll likely miss.

Detect

- Establish a Data Loss Prevention (DLP) program responsible for classifying and tagging data and providing alerts when sensitive or other company-identified relevant information is leaving the organization.
- The DLP program should include an insider-threat detection software that can baseline normal behavior and automate the monitoring of behavioral changes and provide alerts. Technical teams should play an active role in minimizing insider threats.
- Provide anonymous hotlines to report potential abuse and ensure there is no retaliation or action taken against whistleblowers. Show that unauthorized actions have consequences.
- Utilize available access logging for alerts or in quick investigation/triage.

Disrupt

- Establish a robust process to investigate these alerts; pass true positives to the relevant team at your company and track actions taken against offenders. We've seen abuse drop by 80% with minimal resource investment and a strong tone from the top. Solid partnerships between the C-suite, legal, HR, and governance, risk and compliance are critical to success.
- Should an employee be terminated, act quickly to revoke their access (active sessions, tokens, disabling accounts, MFA devices, and rotating credentials), and then verify that access has been revoked. Additionally, ensure you preserve their system and data in case an investigation is needed.

Continued on next page >

INSIDER THREAT PREVENTION PRO TIPS *(continued)*

- When a high-quality alert or indicator of abuse is generated, consider automating your responses until you can catch up. This may include isolating the employee's machine on the network, locking their account, locking access to the data they accessed, and blocking their access attempt in the first place.
- If you think that you have an insider potentially stealing data, quietly begin to investigate, keeping people "in the know" about the investigation to a minimum. Bring in your legal counsel immediately. There are firms with extensive expertise in digital forensic analysis with a focus on insider threats.
- Carefully vet who you hire. Deterring insider threats begins with hiring trustworthy employees.

ABOUT THE CRYPSIS GROUP

Crypsis creates a more secure digital world by providing the highest-quality cybersecurity services to over 2,200 organizations globally, including:

- Data Breach Response
- Cyber Risk and Resilience Management
- Digital Investigations
- Expert Witness and Litigation Support
- Data Analytics and Intelligence
- Managed Security Services
- Hadron (a next-generation endpoint detection and response platform)

Named one of the Top 10 Digital Forensics Services Companies of 2019 by Enterprise Security magazine and one of America's Best Startup Employers, 2020, by Forbes, The Crypsis Group helps clients defend against and respond to cybersecurity threats through their cybersecurity expertise, global incident response capabilities, and continuous innovation. The company has offices in Washington, D.C., New York, Chicago, Austin, and Los Angeles. For more information, visit www.crypsisgroup.com.

twitter.com/crypsisgroup

linkedin.com/company/crypsis/

paloalto® NETWORKS | CRYPSIS™ A PALO ALTO NETWORKS COMPANY

CORTEX™ BY PALO ALTO NETWORKS

paloaltonetworks.com | crypsisgroup.com