ARCTIC WOLF

ARCTIC WOLF

2025 THREAT REPORT

TABLE OF CONTENTS

FOREWORD

This Arctic Wolf® Threat Report draws upon the first-hand experience of Arctic Wolf's security experts, augmented by Arctic Wolf Labs research into the cybercrime ecosystem and additional credited sources.

By deliberately focusing on cyber attacks that escalated to a level of requiring an incident response (IR) investigation by Arctic Wolf, we aim to:

01 **Highlight which attack types are responsible for severe incidents**

02 **Uncover the tactics, techniques, and procedures (TTPs) that allow threat actors to evade detection long enough to pursue actions on objective (e.g., deploying ransomware, tricking organizations into transferring funds, conducting intrusions, etc.)**

03 **Raise awareness of the cybersecurity practices needed to prevent, detect, and recover from such incidents**

Very broadly, we see evidence that threat actors are adapting to target stronger cybersecurity postures by looking for novel methods of attack or embracing low-tech — but effective — means of bypassing high-tech safeguards. At the same time, competition within their own ranks and better resilience on the part of their victims has ransomware operators engaging in more aggressive tactics and taking a firmer stance on ransom payments. Business email compromise (BEC) continues to be a menace, especially for organizations that routinely transfer funds and use email to coordinate these activities. And although many intrusions we investigated appear to be failed ransomware attacks, others are more likely to be incidents of stealthy cyber espionage.

How do organizations protect themselves in the continuing cybersecurity arms race? By focusing on the fundamentals, including:

- An adaptable security posture
- Detection and response spanning the full attack surface
- An IR process and partner that enables fast and effective recovery

Our hope is that reading this report will equip you with insights and actions to bolster all three of these elements.

KERRI SHAFER-PAGE,
Vice President, Incident Response

KEY TAKEAWAYS

95%

THREE CYBER INCIDENT TYPES ACCOUNT FOR 95% OF ALL IR CASES

Organizations typically reserve third-party IR engagements for only the most disruptive and damaging incidents, so it's telling that **our cases are dominated by ransomware (44% of cases), business email compromise (27%), and intrusions (24%)**. While their combined contribution is quite consistent year over year, an increase in the intrusion proportion is largely offset by a decrease in ransomware's share. Detailed analysis hints that this is no mere coincidence, with signs that many ransomware attacks were stopped prior to detonation — indicating that organizations are improving their detection capabilities.

96%

96% OF RANSOMWARE CASES INCLUDED DATA THEFT, AS THREAT ACTORS ADAPT TO STRONGER BACKUP AND RESTORATION CAPABILITIES

As potential victims implemented more reliable backup and restoration processes, ransomware operators introduced data exfiltration as a means to apply additional pressure and protect their revenue streams. Today, this double extortion is undeniably the norm, as **96% of ransomware incidents we investigated included this element**. Nevertheless, preparedness on the part of organizations remains important: our case analysis shows that in 68% of ransomware incidents, backups aided in the recovery process.

+50

THE RANSOMWARE LANDSCAPE IS A MODERN-DAY HYDRA

The well-established ransomware-as-a-service (RaaS) model has democratized access to ransomware software, intrusion tools, and — via initial access brokers — IT environments. One result is a very long tail of threat actors all vying for a piece of the cybercrime pie; as such, **we observed more than 50 unique ransomware threat actors in victim environments**. Like the Hydra of Greek mythology, when a ransomware operation ceases to exist — whether due to law-enforcement operations, infighting, politics, retirement, etc. — other groups (new and old) fill the void.

PROFESSIONAL INCIDENT RESPONSE (IR) PAYS OFF

In the not-too-distant past, most ransomware actors showed at least some willingness to negotiate with the victim to arrive at a workable solution. Nowadays, though, harassment and a stated refusal to negotiate are commonplace. Expert incident responders have encountered all these tactics before. Despite attackers' persistent threats and aggressive tactics, our IR professionals were able to **reduce aggregate ransom demands by 64%**. Perhaps more importantly, our IR expertise was a major reason why 70% of our clients who used our negotiation services did not pay their ransoms. The Arctic Wolf Incident Response team includes a Threat Negotiation team and does not leverage the use of a partner or vendor to complete these activities.

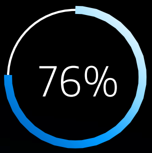
KEY TAKEAWAYS

WHEN IT COMES TO BUSINESS EMAIL COMPROMISE (BEC), FRAUDSTERS FOLLOW THE MONEY

The finance and insurance industry accounted for 26.5% of BEC IR cases, roughly double the second-place industry (legal and government, at 13.3%). In fact, BEC accounted for 53% of IR cases pertaining to finance and insurance — the only industry for which BEC outnumbered ransomware. Clearly, **organizations that regularly exchange money and process payment details over email are in the crosshairs of BEC attacks.**

ATTACKERS EMBRACE LOW-TECH WAYS TO BYPASS HIGH-TECH DEFENSES

Why kick down the door when you already have the key, or can find someone to open it on your behalf, or — best of all — you find it unlocked to begin with? **Unsecured Remote Desktop Protocol (RDP) and compromised VPN credentials are the leading root causes of ransomware and intrusions**, while phishing and previously compromised credentials are behind the vast majority of all BEC cases. Access controls and safeguards including strong, phishing-resistant multi-factor authentication (MFA) can not only help to stop attackers from gaining initial access, but are also effective means of thwarting intrusion actions, including reconnaissance.



PRIORITIZED PATCHING CAN PREVENT INTRUSIONS

In 76% of intrusion cases, threat actors employed at least one of 10 specific vulnerabilities, none of which were zero-days and seven of which were associated with remote access tools or other externally facing services. Vulnerability management can seem like a never-ending game of high-stakes Whac-A-Mole — but a little prioritization can take away attackers' favorite means of infiltration. To inform that prioritization, organizations must understand the complexities of their network, the need to patch critical infrastructure (especially VPN services, firewalls, and other edge devices) based on CVE severity (if known), and the answers to the questions, "Where is our data?" and "Where is our customers' data?"

THREAT ACTORS SAVE THEIR ZERO-DAY EXPLOITS FOR STEALTHY INTRUSIONS

While zero-day exploits almost never appeared in ransomware (0.4% of cases) or BEC (0%) incidents, they represented the fifth-leading root cause in intrusions — accounting for 6% of such cases. This stark contrast suggests **threat actors are selective, reserving such actions for the most sensitive and targeted activities with the highest probability of success**.

INTRODUCTION

The insights and data presented are drawn from hundreds of global digital forensics and incident response (DFIR) engagements conducted by the Arctic Wolf Incident Response team from October 1, 2023, through September 30, 2024.

The IR case data is augmented with telemetry from the Arctic Wolf Aurora Platform and research from our threat intelligence team, digital forensics experts, incident responders, and professional ransomware negotiators.

The top three incident types collectively accounted for 95% of all IR cases.

Accordingly, we will examine these three types in detail to provide an overview of the threat, and:

- Reveal which industries are most impacted
- Understand root causes
- Dive into related topics

Data sourcing and methodology

To enable the holistic analysis within this report, all data is aggregated without any identifying characteristics or attributes.

The vast majority of these IR engagements were initiated as part of cyber insurance policies, through our partnerships with insurance providers and privacy law practitioners. Consequently, these incidents typify cyber attacks that were so severe (i.e., damaging, disruptive) that they led to insurance claims — making them ideal study subjects in our aim to better understand the most dangerous threats.

While cyber insurance is a valuable risk transfer option for any organization, it's important to recognize that certain industries are more likely to have coverage than others, and that our sample cases will reflect this distribution. Rephrased, the sample represents our real-world experience delivering incident response services and is not intended to represent all cyber attacks across all markets and segments.

Case classification

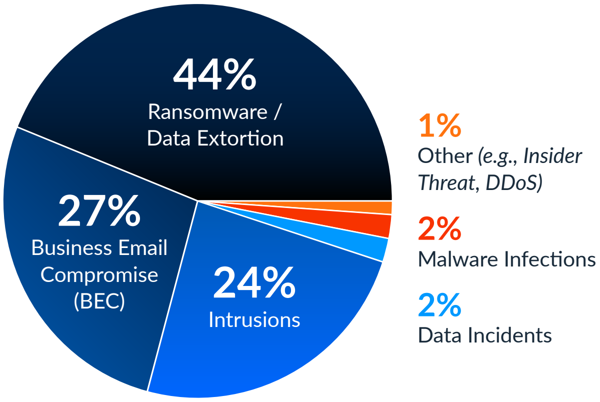
We classify cases by the focal point of the incident, or the best answer to the question, "What is the most impactful aspect of the attack?"

However, many cyber incidents include multiple elements, as threat actors rarely execute a single action. For instance, an attacker may employ social engineering to obtain credentials which are then used to access the environment via a VPN service, followed by lateral movement and reconnaissance, all as precursors to exfiltrating data and ultimately deploying a malicious payload to encrypt files.

If this attack progressed through all those steps, we would classify the incident as a ransomware/ data extortion case; however, if the lateral movement was detected and contained, it would be classified as an intrusion.

Incident Response Cases by Category

(October 1, 2023 through September 30, 2024)



PART 01

PART 01: RANSOMWARE & DATA EXTORTION

Highlights

- **RANSOMWARE REMAINS THE BIGGEST DRIVER OF IR CASES:** 44% of IR cases during the reporting period pertained to ransomware, indicating just how prevalent such incidents are to victimized organizations.
- **AS BACKUP AND RESTORATION CAPABILITIES IMPROVE, DOUBLE EXTORTION IS NOW THE NORM:** In 96% of ransomware IR cases, the attacker also exfiltrated data to apply pressure and extort payment.
- **EXPERT NEGOTIATION IS WORTHWHILE:** Although every case is unique to some degree, Arctic Wolf's experienced ransomware negotiators were able to secure a 64% reduction in aggregate ransom demands.
- **MANY VICTIMS PAY UNNECESSARILY:** While prior surveys suggest that upwards of 80% of victims ultimately chose to pay a ransom, our data shows only 30% of Arctic Wolf IR cases resulted in a ransom payment — and in the majority of those incidents, the victim paid to expedite recovery, rather than out of necessity.
- **ATTACKERS ARE LETTING THEMSELVES IN:** Unsecured Remote Desktop Protocol (RDP) and compromised virtual private network (VPN) credentials are the leading root causes of ransomware IR cases —with RDP alone being the culprit in 38% of such incidents.

For the 12-month period covered by this report, Ransomware / Data Extortion cases accounted for 44% of our IR incidents.

This proportion represents a slight decline from last year's report (48.6%)[1], but nevertheless underscores ransomware's dominance as an attack-of-choice for many threat actors.

Unfortunately, all signs indicate that ransomware and data extortion will remain everyday threats for the foreseeable future. In particular, the risk versus reward calculation provides strong incentives for attackers to go this route. Consider that:

- Despite some high-profile law enforcement takedowns, the chances of perpetrators facing legal consequences remains low (especially when they enjoy the protection of their governments or security agencies)
- Ransom payments, on average, remain high (more on this, in a moment)
- There's always the possibility of a massive payout — for context, 2024 saw the largest ransom payment on record (**$75 million USD** from a Fortune 50 company, paid to the Dark Angels group)

[1] As we'll see later, there's evidence this decline is the result of effective defenses stopping attacks at the intrusion stage (i.e., before ransomware deployment)

PART 01

PART 01: RANSOMWARE & DATA EXTORTION

Lower barriers to entry have led to a crowded landscape

During this reporting period, we observed more than 50 unique threat actor groups operating in victim environments.

This expansive collection is what happens when financial incentives intersect with the democratization of ransomware, the latter of which is the result of the evolving cybercrime ecosystem.

In the early history of ransomware, threat groups managed the entire attack lifecycle in-house. This meant they needed the skills to develop ransomware software, identify potential victims, successfully infiltrate targets, perform intrusion actions leading to ransomware deployment and detonation, and negotiate payment.

Today, **ransomware-as-a-service (RaaS)** is a well-established model in which:

- Ransomware developers (individuals and organizations) write their own software, then lease it to other individuals and groups (usually as a percentage of the ransoms paid)
- Initial access brokers (IABs), who specialize in gaining access and establishing persistence, sell access into IT environments around the globe
- Individuals and criminal organizations, operating as affiliates to the ransomware groups, conduct the actual attacks and negotiations

Now, any aspiring cybercriminal can simply purchase access into an organization from an IAB and then deploy the ransomware. As part of their affiliate relationship with the ransomware authors, the actual attacker may receive general guidance (or even strict rules) about how to conduct the negotiations; they will also be able to leverage the author's reputation, as needed.

Plus, the individuals or groups launching attacks are rarely tied to a single variety of ransomware. Exclusivity agreements are rare (and difficult to enforce), so attackers can pick and choose whichever strain they prefer — whether for some technical reason, or perhaps because they stand to earn a bigger cut of the payday.

'Innovation' in Action

Although it's certainly possible to have file encryption or data extortion, rather than both, 96% of the ransomware cases to which we responded included both elements.

The first known "double extortion" incident occurred in 2019, when the Maze ransomware operation attacked security staffing firm Allied Universal. In addition to encrypting files, Maze exfiltrated sensitive data and threatened to publish it unless Allied Universal paid the ransom.

The model quickly caught on and is now the norm due to the pressure it exerts — including against victims with reliable backup and recovery processes.

Notably, threat actors continue to add new extortion layers, including contacting business partners of victims and family members of executives — anything to compel a quick and large payment.

Learn more in our blog, **The Dangers of Double and Triple Extortion in Ransomware**

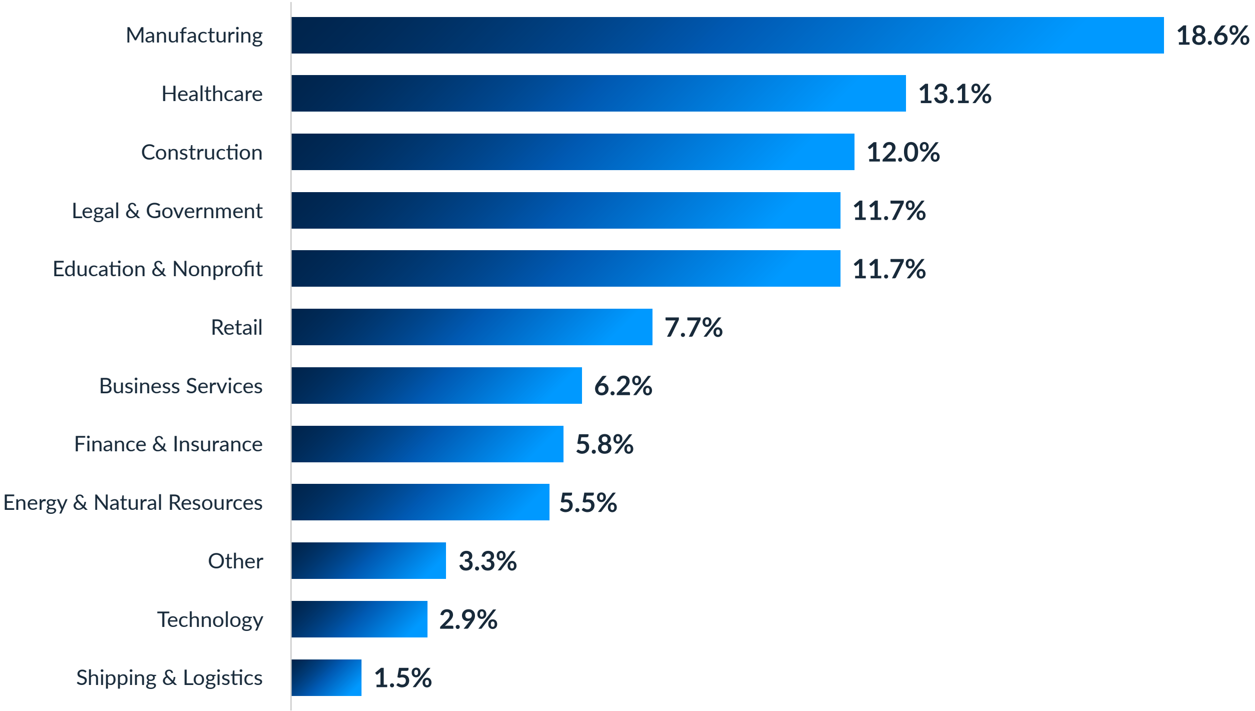
PART 01: RANSOMWARE & DATA EXTORTION

Ransomware actors continue to target organizations with no tolerance for downtime

To extract a payment, ransomware operators apply pressure, typically by taking operations offline or threatening to release sensitive data.

And when we look at the data, we see that five industries that are highly susceptible to both these tactics account for just over two-thirds of ransomware IR cases.

Ransomware & Data Extortion IR Cases by Industry



Manufacturers are historically a favored target of threat actors, as any operational disruption threatens to derail production, risk contractual penalties, create backlogs, and damage the manufacturer's reputation. Plus, manufacturers often hold valuable information about industrial processes and customers, making them similarly susceptible to the data extortion aspect of modern ransomware.

Given this context, it's unsurprising to see the manufacturing industry accounts for the largest share of ransomware IR cases, at 18.6%.

Healthcare has the second-largest share, at 13.1%, followed by construction with 12%. The top five are rounded out by legal and government, and education and nonprofit, each at 11.7%.

Like in manufacturing, service or production outages for organizations in any of these industries become immediately evident and have significant consequences; similarly, many such organizations will also be sitting on troves of sensitive and proprietary data.

PART 01: RANSOMWARE & DATA EXTORTION

Ransoms: demands, negotiations, and potential payment

From an outside perspective, ransomware incidents can seem like fairly simple transactions: an attacker severely disrupts an organization and threatens to release data, the attacker states a ransom amount, the organization pays to expedite recovery or refuses to pay.

Behind the scenes, though, things are considerably more complicated.

THE MEDIAN AGGREGATE RANSOM DEMAND REMAINS AT $600,000 (USD)

It's generally understood that cybercriminals base their initial ransom demand on a multitude of factors, including:

- The victim organization's size and financial position, which threat actors use to estimate the organization's ability to pay
- The victim organization's industry, which influences their sensitivity to disruption and negative press, and which could provide relevant history on frequency of payouts
- The scope of the attack, which typically influences the victim's ability to recover and the impact to their operations
- The victim's insurance coverage, as some ransomware groups actively seek out cyber insurance policies in a victim's environment to better inform their ransom demands
- The ego, mood, and reputation of the attacker

With so many variables at play, there can be considerable variation from year-over-year within each industry. Indeed, comparing the figure below to the one in last year's report reveals only a few strong consistencies:

- Retail and the energy and natural resources sector once again faced the highest median ransom demands
- Healthcare continued to receive the second lowest ransom demands
- Manufacturing and technology were again in the bottom half

The remainder of the list is heavily reordered, compared to last year's report, with the most notable changes being:

- Construction, which was third-lowest last year, has jumped to third highest
- Finance and insurance, which was fourth-highest last year, has dropped to last

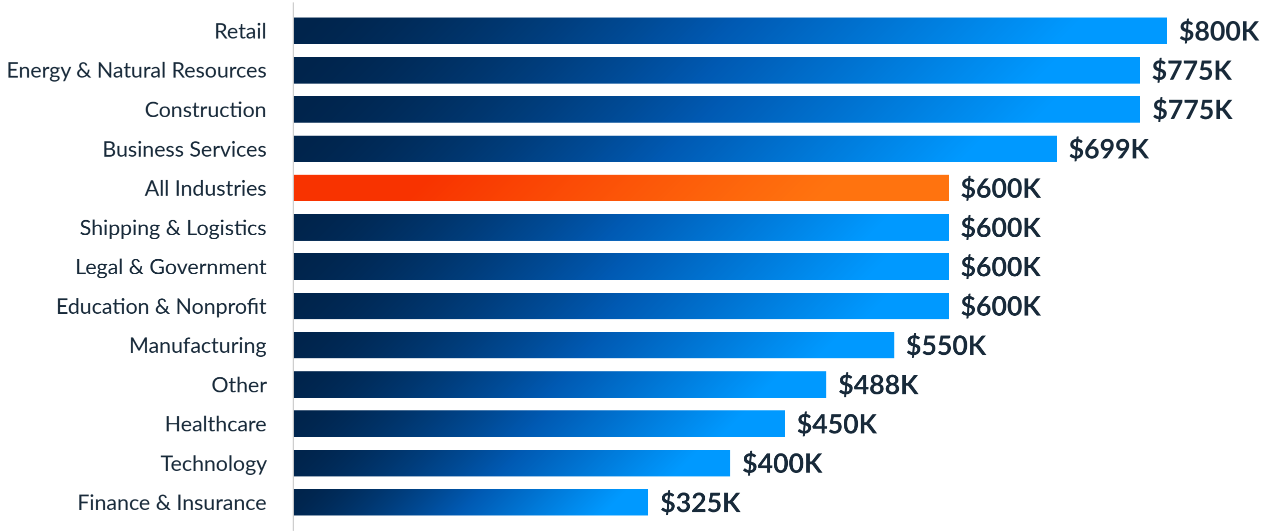
Although it's tempting to posit explanations for both the consistencies and changes, probably the wisest approach is simply to observe that there is tremendous variation across and within industries, and that specific ransom amounts remain largely unpredictable.

In the aggregate (i.e., across all industries), the myriad of variables largely control for themselves, leading to less fluctuation and stronger predictive value. In fact, despite all the shuffling, the aggregate median initial ransom demand is unchanged: $600,000 (USD).

Perhaps the 'ransomware industry' as a whole is reaching something of a steady state, now that victims are better prepared to recover, and now that the cyber insurance market is maturing.

PART 01: RANSOMWARE & DATA EXTORTION

Median Initial Ransom Demand by Industry (USD)



Expert negotiation pays off

Many victims— especially those who choose to respond to an attack on their own without professional support — may not be aware that the ransom demand can be negotiated down.

It's worth bearing in mind that the worst outcome for the attacker is that they don't get paid. A ransom demand that's too high or an outright refusal to negotiate can both increase the odds of this result, so ransomware actors have strong motivations to come to the negotiating table, so to speak.

Although negotiating with criminals is at best unsavory, the harsh business reality is that doing so can pay off in a significant way. Individual cases vary, of course, but our IR case data reveals that, in aggregate – **Arctic Wolf ransomware negotiators were able to reduce the ransom demand by 64%.**

But negotiating with a ransomware actor is best left to the experts, who generally have much, much more experience with doing so than any in-house personnel. A professional ransomware negotiator will work on the victim's behalf to communicate with the threat actor, to better understand the situation, and to try to reduce the amount demanded.

Plus, we've observed that attackers are becoming more aggressive with their extortion tactics and adopting tougher stances. In the not-too-distant past, most ransomware actors showed at least some willingness to negotiate with the victim to arrive at a workable solution[2].

Nowadays, though, harassment has become much more common, and some attackers even reach out to the victim organization's business partners and the families of the victim organization's executives — all while refusing to reduce their demands.

[2] Note: We're not at all giving them credit for this behavior — our intention is merely to contrast this slightly less deplorable behavior with the more aggressive behavior of the recent past

PART 01: RANSOMWARE & DATA EXTORTION

Expert incident responders have encountered all these tactics before.

Still, there's a bigger question: whether or not a threat actor reduces their demand, do victimized organizations even need to pay the ransom?

Ransom payments are often a business decision rather than a recovery necessity

At Arctic Wolf, our position aligns with the general recommendations of the FBI, other law enforcement agencies, and governments: If possible, ransom demands should not be paid, as starving the perpetrators is the only way we can collectively hope to eliminate these attacks.

Nevertheless, the decision on whether to pay is one that must be made by stakeholders within the victim organization once presented with all possible information and options.

As context, Arctic Wolf's **The State of Cybersecurity: 2024 Trends Report** revealed that, within that report's 12-month research window, 83% of ransomware victims paid a ransom[3].

In contrast, in the ransomware IR cases used in the report you're reading now, **only 30% of victims elected to pay — meaning 70% chose not to**, nearly the inverse of the survey-sourced number.

What's behind this stark difference?

Lacking visibility into the incidents reflected in the survey, we can't say for sure. However, we believe it's fair to say that an organization acting on their own almost certainly lacks the experience to understand all the options available and may succumb to pressure from the perpetrators to act quickly — but calling in a professional IR team can unlock more options.

Calling in the Experts

Employing the services of a professional IR organization can have many benefits, including:

- **Preventing further problems:** In some circumstances, the threat actor demanding a payment could be a sanctioned entity or have ties to a terrorist organization. In these cases, any payment to such a group constitutes a crime on behalf of the payee.
- **Insight into the situation and explanation of what options are available:** This can include if a payment is even necessary (sometimes decryption keys are already known) and the reputation of the threat actor. Professional negotiators can sometimes get information from the threat actors (e.g., what data was stolen) that can lead to better-informed decisions.
- **Smaller payments:** While every ransomware affiliate and group is different, professionals know who is more likely to lower their demands, and by how much.

[3] That is, 83% of organizations hit by ransomware paid either some or all of the initial ransom demand. Note, however, that this figure comes from a survey of 1,000 IT and security decision makers and was not limited to incidents that pulled in IR professionals or, more specifically, Arctic Wolf's IR professionals. Nevertheless, it indicates that the large majority of ransomware victims pay, overall.

PART 01: RANSOMWARE & DATA EXTORTION

A Matter of Priorities

Detailed examination of our IR case data suggests that paying a ransom was the victim's only viable recovery option in a mere 12% of cases — meaning that some organizations chose to pay when they didn't (strictly speaking) have to.

The main motivations for doing so were to:

- Prevent publication of stolen data
- Speed up the recovery process

01

Let's first confront the reality that the majority of ransomware attacks include data theft.

In theory, paying up is the only way to prevent publication and, supposedly, to ensure deletion (although, per the callout below, "buyer beware" applies).

However, an IR team may provide compelling evidence that paying the ransom, while perhaps preventing publication, won't guarantee deletion. This fact alone might cause an organization to reconsider.

Or maybe the IR team helps the organization better understand the regulatory ramifications or can uncover information suggesting the exfiltrated data isn't as sensitive or damaging as first feared. Maybe the presence of the IR team simply buys time, and — no longer feeling rushed to act — the organization reconsiders and ultimately decides not to pay. This list is not intended to be exhaustive, but rather to highlight some possibilities.

02

The second major aspect is recovery-centric ransoms — that is, paying to receive a decryption key.

In this case, the IR team might know of a flaw in the encryption algorithm that renders decryption without a key possible. Or maybe the decryption keys are already known from prior incidents or law enforcement actions.

In working with the IR team, perhaps the victim organization finds that their backup and recovery processes are sufficient to negate most of the harm, changing the math that determines the 'value' of making the payment.

So, while every situation is different, aggregate case analysis indicates that bringing in a professional IR team is worthwhile.

“Can we trust a ransomware group to be true to their word?”

This is one of the most common questions ransomware victims ask our IR professionals when considering whether or not to pay the ransom/ extortion demand.

Our best, most-informed answer is roughly, “Generally, yes, but…”

“Generally, yes…”

Most ransomware groups and affiliates model themselves after legitimate businesses; accordingly, they recognize that their success depends in large part upon their reputation.

If a threat actor’s actions lead to a reputation of not delivering on their promises — by failing to deliver a decryption key or releasing data after a ransom is paid — then that undermines the entire extortion business model.

“But…”

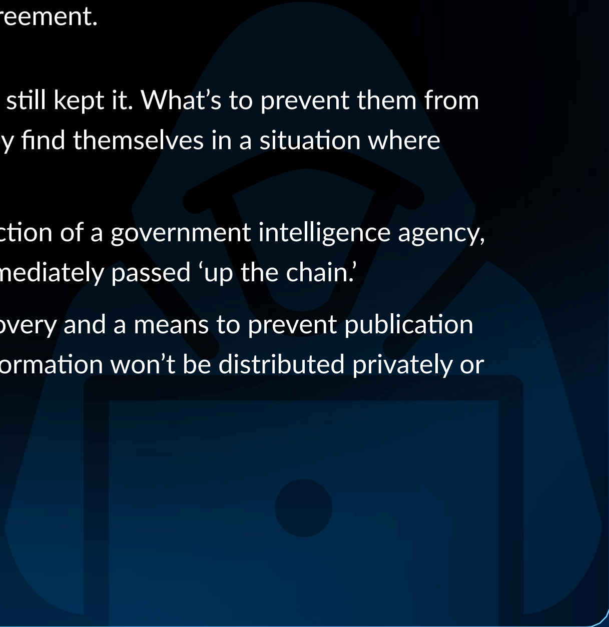
However, although these groups may model themselves as businesses, never forget that they are criminals.

We have handled multiple cases in which our analysts, or agencies with whom we have collaborated, have offensively “hacked back” against the threat actor and discovered data that victims had been assured was deleted — violating the terms of the ransom agreement.

While the threat actor may not have released this data, they still kept it. What’s to prevent them from coming back later and demanding additional payment if they find themselves in a situation where they need more money?

Plus, if the ransomware actor enjoys the patronage or protection of a government intelligence agency, it’s reasonable to presume that exfiltrated information is immediately passed ‘up the chain.’

In general, payment may be regarded as a path to faster recovery and a means to prevent publication of data but should not be considered as a guarantee that information won’t be distributed privately or even that these criminals will stay true to their word.



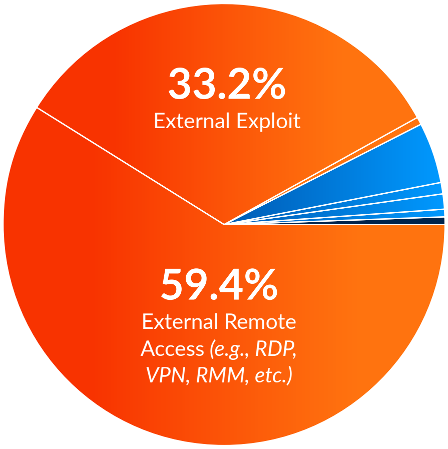
PART 01: RANSOMWARE & DATA EXTORTION

Unsecured RDP is the root cause of the largest portion of ransomware cases

External exposure is the root cause of 93% of our ransomware and data extortion IR cases, with two varieties — external remote access (59.4%) and external exploits (33.2%) — accounting for practically all such incidents.

Behind the scenes, though, things are considerably more complicated.

Root Causes of Ransomware & Data Extortion IR Cases



0.4%	Zero-Day Exploit
4.4%	Malicious Software Download
0.9%	Previously Compromised Account / Credentials
0.9%	Social Engineering *(e.g., Tech Support Scam, Account Creation, etc.)*
0.4%	Phishing
0.4%	Third Party and Supply Chain

CATEGORIES

93.0%	External Exposure
6.6%	Human Risk
0.4%	Trusted Relationship

Digging deeper, attackers leveraged unsecured Remote Desktop Protocol (RDP) and compromised virtual private network (VPN) credentials as their primary methods, with RDP alone being the culprit in 38% of cases.

To put this in perspective, it means attackers abused the very tools organizations have implemented to enable and secure their remote offices and workforces — often by simply logging in to unprotected services.

With many organizations having offices distributed geographically, and with remote — and hybrid-work models here to stay, remote access tools — including RDP, VPN, and remote monitoring and management (RMM) utilities — are workhorses of modern IT infrastructure.

And, unlike many other elements within the tech stack, these tools generally have to be externally accessible.

Unfortunately, absent an added layer of protection such as strong, phishing-resistant multi-factor authentication (MFA), these services also provide a convenient way for threat actors to largely bypass an organization's defenses.

All an attacker needs to do so is obtain a set of active credentials, which can be sourced via phishing, purchased within a cybercrime marketplace, or 'discovered' via an identity-based attack like credential stuffing or password spraying.

The use of a valid account makes it more difficult for organizations to detect the activity as being malicious, which gives an attacker time to pursue their objectives.

Trending Up: RMM Abuse

During this report period, we observed malicious usage of 32 different RMM tools.

There's also a distinct upward trend, with RMM tools being used in 36% of IR cases within the last quarter.

What if a target doesn't have an RMM tool already in place? We observed several instances where the threat actor would send a phishing email with an unauthorized charge/purchase pretext.

The recipients would be directed to a phishing site, the goal of which is to have them download and install ConnectWise ScreenConnect.

In some cases, the victim would even call a support phone number (provided by the attacker) and actually be guided through the download and installation process.

The Black Basta ransomware group is known to employ a similar approach. After following up an email bombing attack by impersonating IT personnel, the group would use Windows Quick Assist to obtain initial access and then turn to a combination of RMM tools to maintain persistence.

Unfortunately, as explained in the **Arctic Wolf Labs 2025 Predictions Report**, we expect threat actors to continue to target perimeter defenses using these same tactics.

To help withstand perimeter-focused attacks, organizations should scan their environments for unsecured RDP and should pay particular attention to credential management (in addition to implementing and enforcing phishing-resistant MFA).

Backing up to bounce back

One of the most effective ways an organization can increase resilience against ransomware attacks is to maintain proper backup practices.

While backups don't address the issues around data exfiltration, being able to restore business operations can buy your organization time and limit the ripple effects of the attack.

Our case analysis shows that in 68% of ransomware incidents, reliable backups aided in the recovery process — in many cases removing the need for a payout by providing an alternate path to sufficient recovery.

Looking beyond ransomware, restoring from reliable backups was also the number one recovery method for intrusions. When an attacker has gained unauthorized access to an environment, there's a high likelihood that they have established multiple persistence mechanisms that would allow them to regain access should they be expelled. Therefore, it's often recommended to restore every system accessed by the attacker and start over, rather than assuming all persistence mechanisms were found and removed — as even a single missed backdoor can prove disastrous.

Outlined below and in the right column of this page are some backup best practices that might make a meaningful difference on a dark day.

Understanding and accounting for the shared responsibility model of cloud services

The cloud/SaaS provider and the SaaS customer (i.e., you) each assume ownership of particular responsibilities with respect to data security. Be sure to understand the terms of each of your contracts, but in general:

- The SaaS provider is only responsible for the underlying application, operating system, virtualization, hardware, and network — including hardware failures, software failures, natural disasters, power outages, and physical intrusion into the data centers
- The customer is responsible for users, data, administration, human errors, programmatic errors, malicious insiders, ransomware attacks, and other malware — in other words, a security incident originating from within your organization that destroys or disrupts your cloud data is your responsibility

Following the 3-2-1 principle of backup

The 3-2-1 principle says that an organization should have:

- 3 copies of data (1 primary and 2 backup)
- 2 different types of media
- 1 off-site copy (ideally in a secure private cloud)

Regular recovery testing

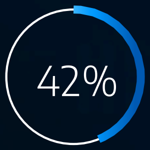
A real-world incident is not the time to uncover problems with processes, prioritization, or the backups themselves — be sure to regularly (and perhaps randomly) test your ability to recover.

Spotlight: The usual suspects

We observed 50 unique ransomware threat actors in victim environments.
The ransomware-as-a-service reality makes positive attribution of an incident considerably more difficult than in years past.

However, such attributions can be informed by a combination of:

- Malware samples
- Infrastructure overlap or reuse
- Post-encryption file extensions
- Ransom messages and leak site postings
- Negotiation script patterns



As such, our team of researchers have identified the five major ransomware groups that were behind 42% of the cases we investigated in the last 12 months.

THREAT ACTOR

AKIRA

DARK WEB DATA:

First Observed:
March 2023

Potential Lineage:
Ryuk > Conti --> Akira

NUMBER OF VICTIMS:

215
*Listed on their leak site**

NUMBER OF POSTS:

19
*Average postings each month on their data leak site***

TOP 3 INDUSTRIES*

01. Manufacturing ~23%
02. Construction ~11%
03. Technology ~7%

TOP 5 COUNTRIES*

01. United States ~51%
02. Canada ~7%
03. United Kingdom ~5%
04. Brazil ~4%
05. Germany ~4%

AW IR DATA | 10.23–10.24:

Percentage of Our Cases:
15%

Median Starting Demand:
$325,000 USD

File Ext. of Encrypted Files:
File extension of encrypted files: .akira or .powerranges (Megazord variant) or .arika when their ransomware misfires / file corruption on hosts

NEGOTIATOR'S TAKE:

"Akira doesn't often stray from their predecessor's procedures, oftentimes we see consistent timing of communications, repeated messages, and similar actions across several cases. They follow a quintessential playbook, so we expect a fairly standard back-and-forth negotiation with them."

*During report timeframe
**Number of victims that have not paid/negotiated

THREAT ACTOR

LOCKBIT 3.0

DARK WEB DATA:

First Observed:
January 2020

Potential Lineage:
ABCD > LockBit > LockBit 2.0 > LockBit 3.0 > LockBit Green > LockBit 4.0

NUMBER OF VICTIMS:

775
*Listed on their leak site**

NUMBER OF POSTS:

65
*Average postings each month on their data leak site***

TOP 3 INDUSTRIES*

01. Manufacturing ~20%
02. Construction ~10%
03. Legal & Government ~9%

TOP 5 COUNTRIES*

01. United States ~41%
02. United Kingdom ~7%
03. France ~5%
04. Germany ~4%
05. Canada ~3%

*During report timeframe
**Number of victims that have not paid/negotiated

AW IR DATA | 10.23–10.24:

Percentage of Our Cases:

9%

Median Starting Demand:

$1,000,000 USD

File Ext. of Encrypted Files:
.lockbit or 8-9 random alphanumeric characters

NEGOTIATOR'S TAKE:

*"This group was established a while back, making them a notorious player in the space. Due to sanctions concerns since Operation Cronos,*** brokers and organizations at large have prohibited payments to this threat group, leaving them struggling to keep up their attacks and affiliates. Since this disruption, it's clear that not all Lockbit threat actors are at the same level of skill or experience in ransomware and their negotiation tactics are not consistent."*

****Operation Cronos (late-February 2024) involved the seizure of the group's infrastructure (including their leak site), 34 servers, the closure of 14,000 rogue accounts, and the freezing of 200 cryptocurrency accounts, and five indictments against members of the group.*

LOCKBIT

THREAT ACTOR

BLACK SUIT

DARK WEB DATA:

First Observed:
May 2023

Potential Lineage:
Ryuk > Conti > Zeon > Royal > BlackSuit

NUMBER OF VICTIMS:

116
*Listed on their leak site**

NUMBER OF POSTS:

10
*Average postings each month on their data leak site***

TOP 3 INDUSTRIES*

01. Manufacturing ~15%
02. Construction ~15%
03. Healthcare ~13%

TOP 5 COUNTRIES*

01. United States ~71%
02. United Kingdom ~7%
03. Canada ~5%
04. Belgium ~2%
05. Netherlands ~2%

AW IR DATA | 10.23–10.24:

Percentage of Our Cases:

6%

Median Starting Demand:

$650,000 USD

File Ext. of Encrypted Files:
.blacksuit

NEGOTIATOR'S TAKE:

"In our experience, this group is highly likely to resort to a very specific scare tactic – calling a victim on the phone with an ominous message, particularly right at the beginning of a negotiation. While this tactic does instill fear, we encourage victims to remain calm knowing this is their standard practice. Since they rely so heavily on this scare tactic, they may not respond daily in actual negotiations, with delays in communication up to several days on their part."

*During report timeframe
**Number of victims that have not paid/negotiated

THREAT ACTOR

< FOG />

DARK WEB DATA:

First Observed:
May 2024

Potential Lineage:
Ryuk > Conti > Akira --> Fog

NUMBER OF VICTIMS:

21
*Listed on their leak site**

NUMBER OF POSTS:

7
*Average postings each month on their data leak site***

TOP 3 INDUSTRIES*

01. Education ~38%
02. Manufacturing ~19%
03. Food & Beverage ~2%
(tied with construction)

TOP 5 COUNTRIES*

01. United States ~57%
02. Canada ~10%
03. Netherlands ~9%
04. Australia ~9%
05. Germany ~5%

AW IR DATA | 10.23–10.24:

Percentage of Our Cases:
5%

Median Starting Demand:
$610,000 USD

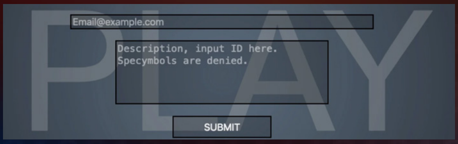
File Ext. of Encrypted Files:
.fog or .flocked

NEGOTIATOR'S TAKE:

"Since we first encountered and brought this group in the spotlight earlier this year, Fog has proven to act as a new kid on the block loosely following in Akira's footsteps. Fog threat actors often don't seem to have the full Akira "playbook" quite yet, with conversations taking a much less professional tone and not behaving the way a more established group would."

*During report timeframe
**Number of victims that have not paid/negotiated

THREAT ACTOR



Email@example.com

```
Description, input ID here.
Specymbols are denied.
```

DARK WEB DATA:

First Observed:

June 2022

Potential Lineage:

Play

Potential affiliation to Hive and/or Nokoyawa

NUMBER OF VICTIMS:

386

*Listed on their leak site**

NUMBER OF POSTS:

32

*Average postings each month on their data leak site***

TOP 3 INDUSTRIES*

01. Manufacturing ~19%

02. Construction ~18%

03. Technology ~6%

TOP 5 COUNTRIES*

01. United States ~77%

02. Canada ~7%

03. United Kingdom ~4%

04. Germany ~3%

05. Netherlands ~2%

AW IR DATA | 10.23–10.24:

Percentage of Our Cases:

4%

Median Starting Demand:

$5,595,000 USD

File Ext. of Encrypted Files:

.play

NEGOTIATOR'S TAKE:

"An extremely stubborn and bull-headed group to negotiate with. They start with ridiculously high demands and are not likely to budge before resorting to scare tactics like phone calls and other communications to victims. Despite these tactics, there are often delays in communication from this group in negotiations"

*During report timeframe

**Number of victims that have not paid/negotiated

PART 02

PART 02: BUSINESS EMAIL COMPROMISE

Highlights

- **BEC INCIDENTS ARE THE SECOND-LARGEST CAUSE OF IR CASES:** 27% of IR cases during the reporting period pertained to BEC, consistent with last year's report (29.7%).
- **THREAT ACTORS FOLLOW THE MONEY:** The finance and insurance industry accounted for 26.5% of BEC IR cases, roughly double the second-place industry (legal and government, at 13.3%).
- **PHISHING AWARENESS AND ACCESS CONTROLS ARE STRONG PREVENTATIVE MEASURES:** Phishing (72.9%) and previously compromised credentials (18.8%) are the leading root causes of BEC cases, pointing to employee training, credential management, and biometric- or possession-based MFA as effective defenses.

Business email compromise (BEC) is a type of email-borne phishing fraud in which a threat actor attempts to trick members of an organization into transferring funds, sensitive data, or something else of value.

Initially, the term strictly referred to account takeover (ATO) incidents in which a threat actor gained access to a legitimate email account within an organization and, masquerading as the account holder, convinced one or more people within that organization to perform some action benefitting the attacker — usually transferring funds to an account controlled by the threat actor.

While the term itself has stuck, its meaning has now evolved to include (i.e., in addition to the ATO scenario):

- Incidents in which a threat actor convincingly impersonates a trusted email contact (as distinct from compromising their account), for instance by using a domain that, at a glance, looks like an organization known to the target[4]
- A longer list of scams or desired outcomes (see the callout on the next page)

[4] At Arctic Wolf, we have more insight into the ATO variety of BEC attack, as the invasive aspect of such incidents makes them more likely to lead to an IR engagement

A Worrying Trend

We have observed some BEC threat actors conducting activities that go beyond email trickery.

For example, multiple threat actors have used applications like PerfectData to integrate with Microsoft 365 — enabling them to exfiltrate the entire contents of the inbox and included data such as emails, attachments, calendar invites, and contacts.

Financial services organizations are the prime targets

During the 12-month reporting period, BEC was the primary impacting factor in 27% of our IR incidents — consistent with last year's report (29.7%).

The industry with the most representation in our BEC IR cases is finance and insurance, which made up 26.5% of the case count. In fact, BEC accounted for 53% of IR cases pertaining to finance and insurance — the only industry for which BEC outnumbered ransomware.

PART 02: BUSINESS EMAIL COMPROMISE

Although BEC scams have expanded beyond seeking to initiate fraudulent transfers, that type of attack still presents the possibility of a large payday for comparatively little effort. Consequently, organizations that regularly shift money around and exchange payment details over email will likely continue to attract a disproportionate share of attention from BEC threat actors.

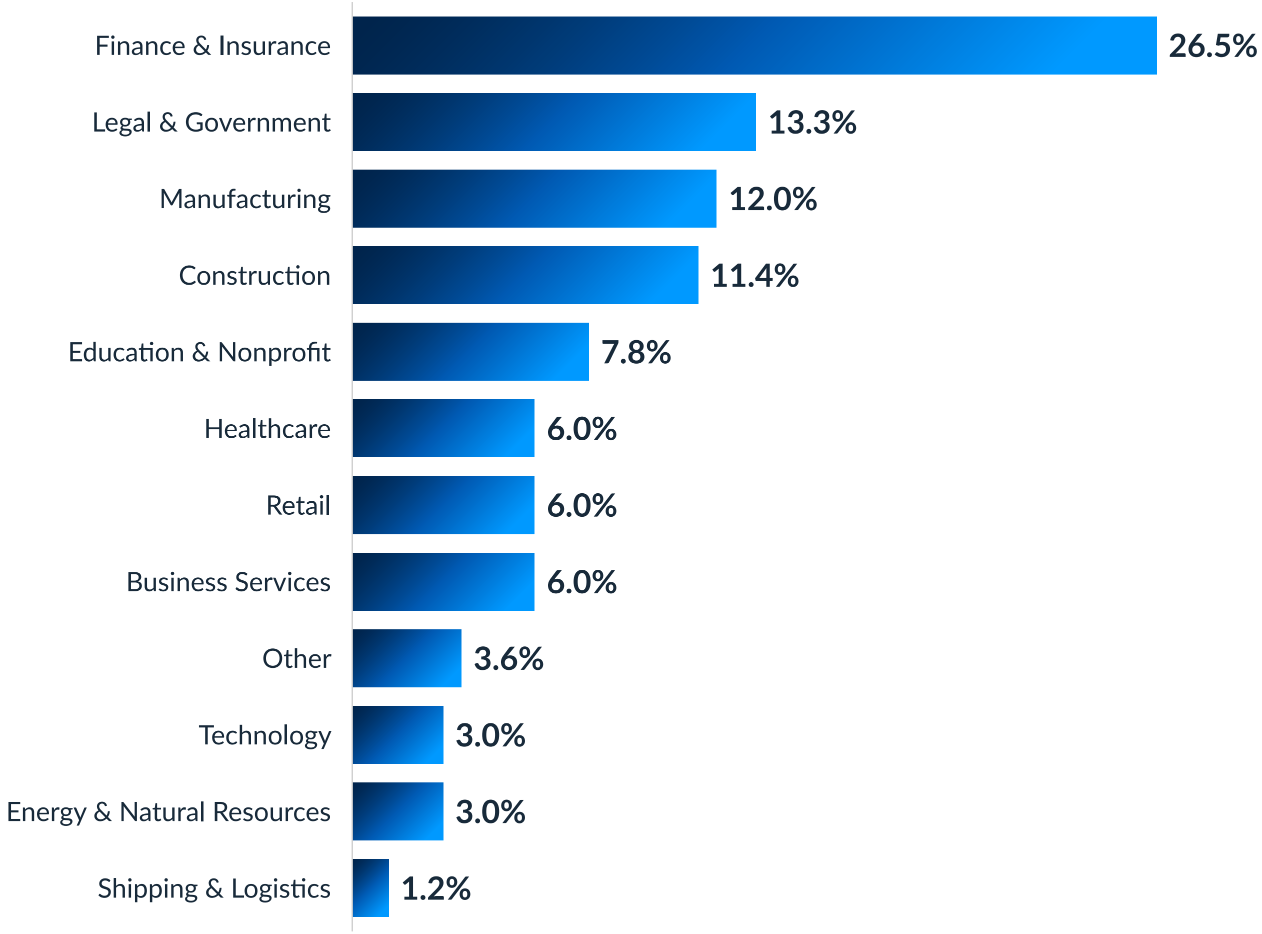
Sutton's Law

As the story goes, a reporter once asked bank robber Willie Sutton why he robs banks.

Not missing a beat, Sutton is said to have replied, *"Because that's where the money is."*

Although Sutton himself claimed the exchange never happened, it's too good for history to forget. It also spawned Sutton's Law, which states that when seeking an answer, one should first consider the obvious.

Business Email Compromise IR Cases by Industry



BEC is more than money transfers and more than account takeovers

BEC fraud comes in many forms (some of which overlap), all of which abuse the implicit trust placed in known contacts and authorities.

At present, these six types represent the most significant threats:

ACCOUNT COMPROMISE

In this classic form (which also gives rise to the BEC synonym email account compromise, or EAC), rather than simply masquerading as a trusted email account, an attacker succeeds in gaining access to an entire legitimate email account and uses it to execute the scam by sending and replying to emails from the hijacked account, sometimes using filtering tools and other techniques to prevent the real account holder from noticing the activity.

FALSE-INVOICE SCHEME

An attacker posing as a known vendor or supplier emails an individual with the authority to transfer funds, transfer to an account controlled by the attacker.

DATA THEFT

An attacker targets HR and finance employees to obtain personal or sensitive information about individuals within the company, such as CEOs and executives. This data can then be leveraged to enable future cyber attacks.

In rarer instances, an attacker masquerading as a customer or vendor may ask a recipient (e.g., in a legal or technical role) to send intellectual property or other sensitive or proprietary information.

PRODUCT THEFT

A relatively new twist, in which an attacker imitating a customer tricks an organization into selling (and shipping) a large quantity of product on credit.

CEO/EXECUTIVE FRAUD

An attacker masquerading as the CEO or other senior executive within an organization emails an individual with the authority to transfer funds, requesting a transfer to an account controlled by the attacker.

ATTORNEY IMPERSONATION

An attacker impersonates a lawyer or legal representative for the company and emails an employee requesting funds or sensitive data. Lower-level employees are commonly targeted through these types of BEC attacks.

Social engineering (phishing in particular) drives BEC cases

Unsurprisingly, given the email-borne nature of the threat, phishing was found to be the primary root cause of BEC cases, accounting for 72.9% of such incidents.

Phishing offers the path of least resistance in the BEC context, as a well-crafted email can trick a victim into performing actions that benefit the attacker — whether directly fulfilling the goal (e.g., transferring funds) or executing an intermediary step (e.g., providing credentials that the attacker can subsequently abuse).

But note, also, the significant contribution of previously compromised account/credentials. These are cases in which a threat actor stole, bought, or found credentials and used these to log in to some application or system within the IT environment. In some cases, they simply logged in to the email service itself. As we note elsewhere, strong MFA should be considered standard practice nowadays, as it can dramatically reduce exposure to credential-related threats. Organizations should also implement strong identity and access management (IAM) practices to protect credentials and should monitor the dark web for dumps that indicate credentials have been compromised.

Circling back to phishing, email lures in the early days of this threat often bore recognizable characteristics like poor formatting, unnatural language (e.g., from non-native speakers or poor machine translation), or kludgy instructions.

However, today's large language models (LLMs) are allowing attackers to quickly and efficiently generate high quality persuasive phishing lures that are nearly indistinguishable from authentic emails. We expect continued evolution in attackers' ability to bypass phishing filters and trick recipients with both:

- General lures, based on high-profile world or industry news, or on generic business matters (e.g., "New vacation policy")
- Targeted spear-phishing leveraging open-source intelligence (OSINT) and information gathered from previous breaches (of the target or of organizations with close ties)

Root Causes of Business Email Compromise IR Cases

73.5%	Phishing
18.9%	Previously Compromised Account / Credentials
4.5%	Email Spoofing
2.3%	Social Engineering *(e.g., Tech Support Scam, Account Creation, etc.)*
0.8%	Malicious Insider

99.2% Human Risk **0.8%** Malicious Insider

Outlook Not So Good

Microsoft continues to have strong market share among businesses — and especially among enterprises (prime targets of cybercriminals).

Accordingly, many phishing campaigns employ clones of the Office 365 login page.

For example, beginning in July 2024, Arctic Wolf identified a new and novel credential theft campaign that typically begins with a phishing pretext to trick the user into opening a link (e.g., an email prompting users to scan a QR code to set up two-factor authentication). The link opens a spoofed Office 365 sign-in page, into which the victim enters their credentials and MFA passcode. The attacker reads this information — acquiring the credentials and MFA passcode — and uses Axios (a JavaScript library used to make client/server requests) to forward requests and responses between the spoofed and legitimate Office 365 pages, so that the victim doesn't become aware that anything is amiss.

As of the date of this report, this campaign is still ongoing.

Combating social engineering

While every social engineering attack may differ in the specifics, each follows the same four-part process:

01 Information gathering: The threat actor researches the target to find what weakness and medium will work best for the attack. Scammers commonly use OSINT and information gathered from prior intrusions to learn as much about the target organization and individuals as possible.

02 Establishing a relationship: The threat actor prepares the foundation of the attack. It could involve targeting a specific department with a phishing message (e.g., email, voice, text) or impersonating an individual (say, the assistant to the CEO) — whatever is deemed most likely to succeed.

03 Exploitation: The attack itself. It may be a high-pressure email purportedly from a person in authority, made all the more believable by referencing a real customer relationship (perhaps learned by reading a press release or perusing LinkedIn).

04 Execution: The scammer's objectives are achieved.

In addition to technical measures like phishing-resistant MFA, preventing social engineering attempts from succeeding requires ongoing training — not once a year — to help your team recognize sometimes subtle signs and to listen to that voice or instinct that suggests something isn't quite right.

Strong security awareness training includes:

- Up-to-date content, relevant to your organization's industry
- Empowering language that treats users as a key element of the organization's cybersecurity strategy, rather than a weak link
- Phishing simulations to track progress and test skills
- Microlearning for better retention and understanding
- Education that builds an organization-wide culture of security

Ideally, the leadership team will set an example by taking cybersecurity seriously, embodying best practices, and avoiding the type of time-sensitive, high-pressure tactics that scammers employ.

PART 03: INTRUSIONS

Highlights

- **INTRUSIONS ARE THE THIRD-LEADING FACTOR BEHIND IR CASES:** 24% of IR cases during the reporting period pertained to network or host-based intrusions.
- **PRIORITIZED PATCHING CAN PREVENT INTRUSIONS:** In 76% of cases, threat actors employed one or more of 10 specific vulnerabilities, seven of which were associated with remote access tools or other externally facing services.

Intrusions were the final leading cause of incident response, accounting for 24% of our IR cases — a significant increase over last year's 14.8%.

It's important to note that the "intrusions" umbrella includes two subcategories:

- **Network intrusions,** in which attackers exploit vulnerabilities in network infrastructure — targeting traffic, protocols, and edge devices (e.g., firewalls, routers, and gateways) to gain access, disrupt traffic flows, or intercept data
- **Host-based intrusions,** which focus on endpoint systems — exploiting software, operating systems, or user accounts for direct system compromise, malware installation, or data theft

Intrusions, the first step towards greater threats

Compared to ransomware and BEC, the industry breakdown of IR cases for intrusions isn't as top-heavy.

Rather, we see three industries — finance and insurance, education and nonprofit, and legal and government — each of which accounts for roughly 15% of the caseload.

Interestingly, the set of the top six industries for intrusions is the same as the set of the top six for ransomware, albeit in a different order.

Key Terms

Intrusion (/inˈtro͞oZH(ə)n/)
noun: *The unauthorized access or exploitation of a weakness by a threat actor for the purposes of gaining access to a network, system, or data*

Vulnerability (/ˌvəln(ə)rəˈbilədē/)
noun: *A weakness within a system or software, whether it's part of the source code or a misconfiguration of settings, that could be exploited by a threat actor allowing them to gain unauthorized access or take malicious actions*

While such overlap could merely indicate that organizations within these industries are regarded as valuable targets in general, it could also suggest that a significant proportion of intrusion cases would have progressed to ransomware deployment and detonation if the intrusion hadn't been detected and contained — strongly underscoring the importance of reactive cybersecurity capabilities.

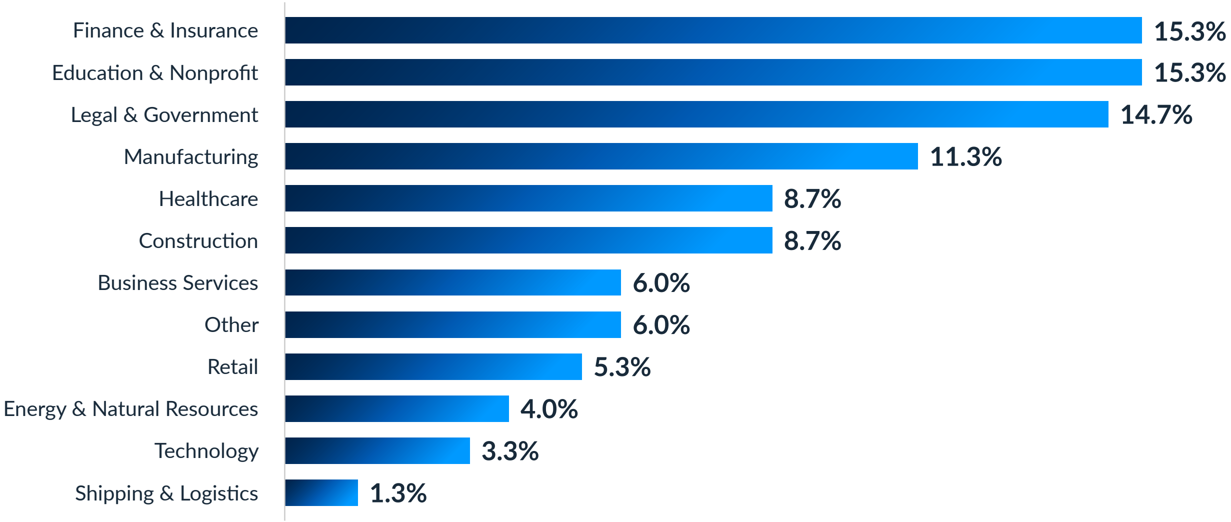
A Trio of Targets

Three industries appear in the top 5 list (by case count) for each of our three main attack types:

- Education & Nonprofit
- Legal & Government
- Manufacturing

PART 03: INTRUSIONS

Intrusion IR Cases by Industry



Intruders disproportionately leverage a small number of vulnerabilities

Like many clichés, the threat landscape being described as dynamic, ever-changing, or ever-evolving is rooted in real-world truth.

New vulnerabilities are constantly being discovered, new exploits — including potentially devastating zero-days — are always being written, and threat actors are always refining their approaches. However, across all IR cases, time and again, we observe attackers leveraging a favored subset of TTPs.

For example:

- In 76% of cases, threat actors employed one or more of 10 specific vulnerabilities (whether to gain initial access or to perform subsequent intrusion actions)
- In 51% of cases, threat actors employed one or more of the top four.

This reality is both:

- Humbling, because patches exist for all 10; and
- Empowering, because it shows that a small amount of prioritized patching can significantly decrease an organization's chances of becoming a victim.

AI-Assisted Vulnerability Discovery

The number of known vulnerabilities continues to climb rapidly, from just under 6,500 in 2015 to more than 40,000 in 2024.

With advances in AI — reasoning techniques, in particular — we expect threat actors to identify novel routes to initial access.

Thus far, even the most advanced AI models have failed to replicate human reasoning capabilities, but that may soon change. Once it does, threat actors will undoubtedly harness this newfound power to uncover new ways to break into protected environments.

Learn more about what we think the near-term future holds in our Arctic Wolf Labs 2025 Predictions Report.

PART 03: INTRUSIONS

Vulnerabilities keep increasing

In another record-setting year, over 40,000 vulnerabilities were recorded in 2024.

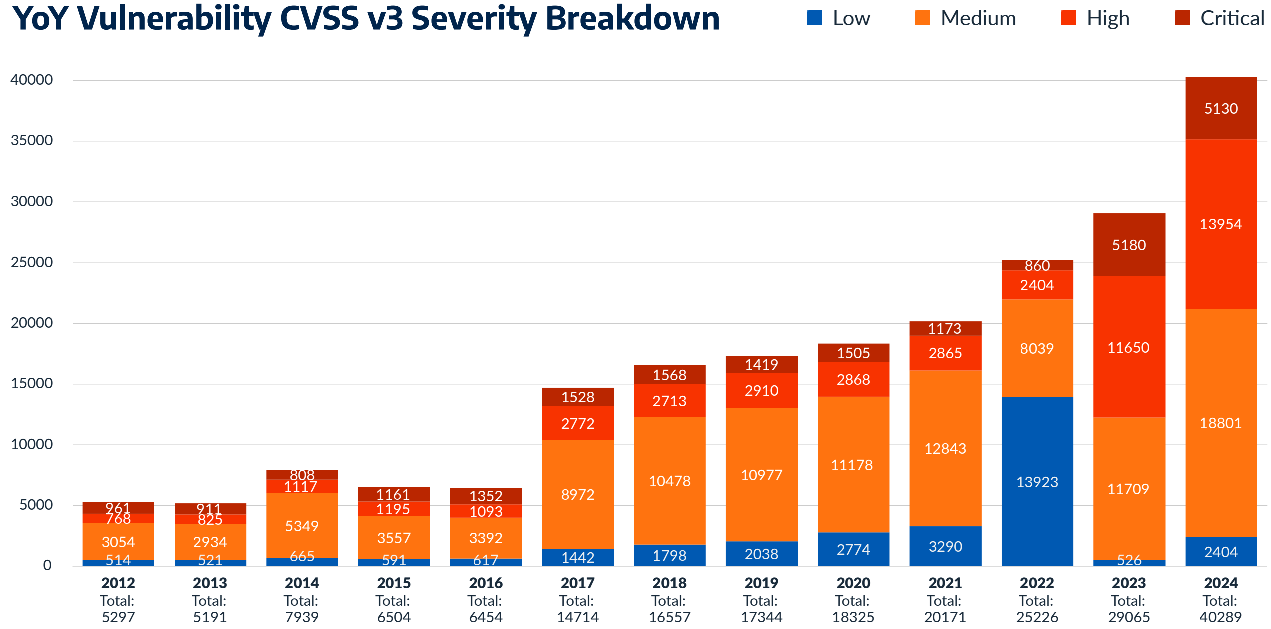
In addition to that alarming number, 2024 was also a record-breaking year in regard to the volume of critical and high-severity vulnerabilities. Both increased by 13.46% in 2024.

This continued growth, fueled by hybrid work models, increasing reliance on web applications, and the use of AI by threat actors, underscores the importance of implementing a robust, risk-based vulnerability management program.

Explore the 2024 vulnerability landscape in-depth and learn how to better protect your organization.

#01	CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability
#02	CVE-2023-4966	Citrix NetScaler ADC & Gateway Buffer Overflow Vulnerability
#03	CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability
#04	CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability
#05	CVE-2023-48788	FortiClientEMS Remote Code Execution Vulnerability
#06	CVE-2023-3519	Citrix ADC, Citrix Gateway/ Citrix Bleed Remote Code Execution Vulnerability
#07	CVE-2023-41266	Qlik Sense Remote Code Execution Vulnerability
#08	CVE-2023-20269	Cisco ASA Firewall VPN Authentication Vulnerability
#09	CVE-2021-31207	ProxyToken: On-Premises Microsoft Exchange Authentication Bypass Vulnerability
#10	CVE-2023-27532	Veeam Backup and Replication Authentication Vulnerability

YoY Vulnerability CVSS v3 Severity Breakdown



Protecting your organization against vulnerabilities

Vulnerability remediation is the act of removing a vulnerability through patching or another process.

By focusing on remediation, organizations can greatly reduce their cyber risk and prevent threat actors from utilizing vulnerability exploits as an attack vector.

There are four main questions an organization needs to ask itself as it sets out to conduct vulnerability remediation:

01 Which vulnerabilities should I remediate first?

02 How can I efficiently remediate those vulnerabilities?

03 How do I prioritize vulnerabilities based on my resources and business risk tolerance?

04 How do I set realistic deadlines for my vulnerability remediation plan?

Of course, those questions are easier to ask than to answer, and for many organizations that lack resources, time, or budget, vulnerability remediation can seem like an endless mountain to climb.

Compounding the challenge, it's difficult to determine which vulnerability to remediate first if you don't have a clear understanding of your overall attack surface. Plus, efficient remediation is all but impossible without contextualization of your entire environment.

Unfortunately, that contextualization — including your risk policies, asset context, and service level objectives (SLOs) — is not easy to achieve when you have limited resources and an overwhelmed IT team. Not to mention the time and resources needed to conduct security scans and do the actual remediating.

That's why remediation should just be one part of a full vulnerability management program, which prioritizes continuous vulnerability remediation and assessment, with other components of the program complementing and assisting overall remediation and mitigation.

PART 03: INTRUSIONS

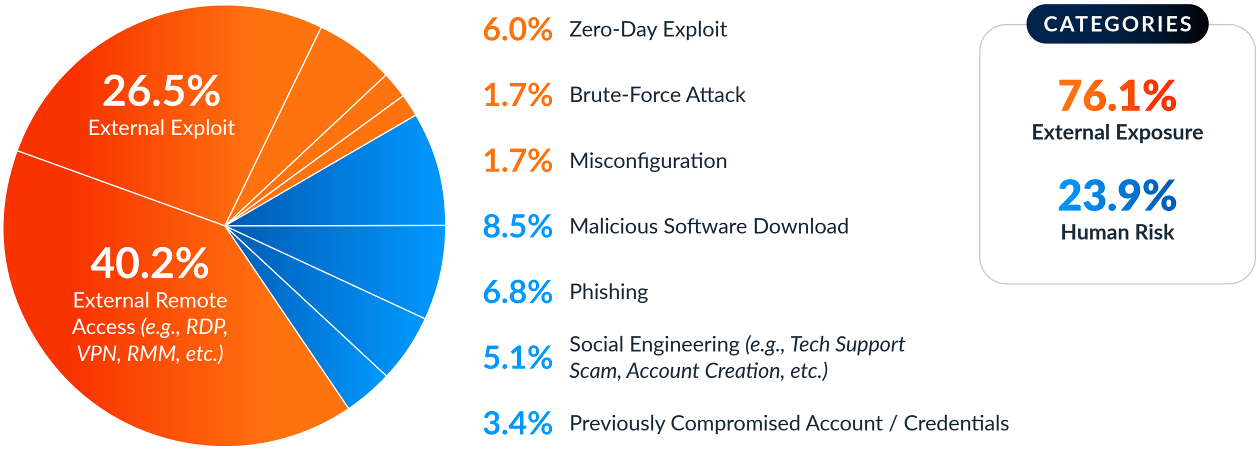
External exposure is the root cause of the vast majority of intrusions

Over half (60%) of intrusions were ultimately traced to external exposure. Like the ransomware cases examined earlier, most of these are attributable to:

- External remote access tools and services (38%)
- External exploits (22%)

The same general analysis and recommendations already discussed (in the ransomware section) with respect to external remote access tools and services apply here.

Root Causes of Intrusion IR Cases



When external exploits were the culprit, the threat actor exploited a vulnerability for which a patch was available prior to the incident — notice that seven of the top 10 vulnerabilities listed above pertain to either remote access tools or externally facing services.

Interestingly, intrusion cases have by far the highest attribution to zero-day exploits (6%, versus only 0.4% for ransomware and no BEC cases).

In some instances where remote access tools were abused, attackers took advantage of misconfigurations (e.g., open ports, externally facing internal websites, administrative accounts vulnerable to brute-force tactics) to gain entry.

It's also worth mentioning that user-initiated malicious software downloads also account for a larger percentage of intrusion cases (8.5%) than they do for either ransomware (4.4%) or BEC (0%). These intrusions may well be opportunistic, in that a threat actor has booby-trapped an application and is simply waiting to be alerted when it's activated within an organization. This approach could be somewhat targeted to particular industries by compromising particular types of software or employing watering hole techniques to attract downloads from certain industries or professional roles.

How to manage the risks associated with credential theft

Credential theft is the stealing of passwords, usernames, or other information that allows for access to networks, applications, assets, or accounts.

Cybercriminals employ several ways to acquire credentials, including:

01 Phishing (e.g., email, voice, SMS)

02 Infostealer malware and credential dumping tools (e.g., Redline Stealer, Mimikatz, Sassy)

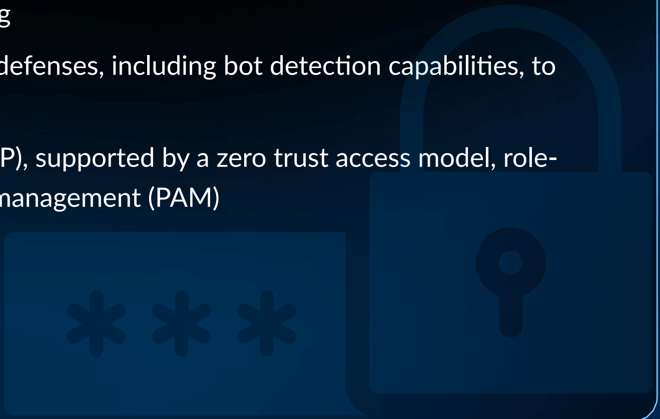
03 Credential stuffing and other brute-force attacks against the login box or API

For organizations with hundreds or thousands of users, staying on top of credential protection can be an overwhelming task, especially if those users are not security minded and are using personal accounts on company devices or a work email address for personal accounts.

Nevertheless, there are proactive and reactive measures a security team can take to improve credential security and to build resilience against threat actors equipped with valid credentials.

These measures include:

- Implementing (and enforcing) strong, phishing-resistant MFA, for example using FIDO Alliance's FIDO2 specifications (e.g., WebAuthn)
- Proactively hardening Active Directory using tools like PingCastle for visibility into configuration weak spots
- Using around-the-clock, real-time monitoring — like the kind offered by a managed detection and response (MDR) solutions — to recognize unusual user behaviors
- Delivering comprehensive employee security training
- Ensuring login services include layers of specialized defenses, including bot detection capabilities, to guard against identity attacks
- Embracing the principle of least privilege access (PolP), supported by a zero trust access model, role-based access control (RBAC), and privileged access management (PAM)
- Conducting (or subscribing to) dark web monitoring



PART 04

PART 04: MANAGING & MITIGATING THREATS

A robust cybersecurity strategy is one that is not only tailored to each organization's needs, but one that also includes both proactive and reactive elements to limit the number and severity of incidents while providing a strong recovery capability.

We've already covered:

- The importance of reliable backup processes, especially for recovering from ransomware and intrusions
- How to build resilience against social engineering, which remains a major root cause of IR cases
- Why prioritized vulnerability management can make it much harder for attackers to achieve their objectives
- How to manage the risks associated with credential theft, which is crucial as threat actors increasingly turn to credential abuse as a means of avoiding defenses

Here are some additional recommendations to help safeguard your organization in 2025.

Develop a solid understanding of your IT environment and attack surface

One of the most important pillars of an organization's security posture is understanding the full breadth and depth of the attack surface.

This data enables organizations to prioritize and refine their security program with precision and develop a stronger vulnerability and security posture management program.

- ☐ **Create and maintain an approved software list:** This helps you rein in shadow IT and (with monitoring) identify intrusions. For example, if software not on the approved list is downloaded within the environment, alert and triage the finding — especially if it's an RMM tool.
- ☐ **Create an inventory of assets and their exposure:** By doing so, you can gain a better understanding of the overall attack surface and can correct instances where applications and devices are mistakenly exposed.
- ☐ **Do not expose management interfaces to the Internet:** We have seen a multitude of vulnerabilities that would have a significantly lower impact if management interfaces weren't exposed.
- ☐ **Take control of the cloud:** We asked an Amazon Web Services expert for their advice on how to best take control of you cloud environment:

> *"From my perspective, many cloud security incidents are not rooted in vulnerabilities but instead can be traced back to misconfigurations and/or overly permissive access policies. You should leverage IAM least privileges policies and monitor configuration drift away from your security baselines as a part of your standard operations."*
>
> – Ryan Orsi, WW Cloud Foundations Partner Specialists

Ensure you have broad visibility (monitoring) into your environment and assets, and create a baseline of normal behavior

Arctic Wolf has consistently recognized that a lack of visibility allows security threats to go unnoticed for far too long.

Expanding environmental visibility beyond endpoints alone increases the likelihood of detecting potential threats at an early stage, allowing for those threats to be stopped before they have a chance to inflict significant damage.

- ☐ **Monitor logs:** Log monitoring is critical to detect major threats. This includes logs from intrusion detection systems (IDS)/network detection and response (NDR) systems, endpoint detection and response (EDR) solutions, firewalls, identity and access management (IAM) systems, email services (e.g., to monitor for changes in access and the creation of filtering rules), and the cloud-hosted services that extend your organization's environment beyond your own infrastructure.
- ☐ **Monitor endpoints:** Implementing endpoint monitoring across the environment will help you review public ports, disable unnecessary ports, and restrict port destinations. This type of monitoring is crucial to provide visibility into actions taken by potential threat actors. While other types of log sources can complement this type of visibility, they cannot replace it.
- ☐ **Create a baseline:** The better your understanding of your environment, the better positioned you are to spot deviations that could be signs of a cyber attack, including data exfiltration.

Enforce strong identity controls

Identity is becoming a major battleground in modern cybersecurity, and today's threat actors are adept at finding and leveraging credentials that allow them to log into services and move unnoticed around victim environments.

- ☐ **Implement and require strong, phishing-resistant MFA:** At this point, failing to implement MFA can be seen as an unnecessarily risky decision. Similarly, relying on legacy MFA techniques introduces further unnecessary risk while giving a false sense of protection. Safeguarding your organization requires modern, phishing-resistant MFA (e.g., based on the FIDO2 set of specifications).
- ☐ **Employ a zero trust security strategy:** Zero trust limits all access unless identity and security posture can be verified. This strategy can reduce the attack surface and limit an attacker's ability to move laterally through an organization's network.

Establish and continually foster a culture of security

Positive security outcomes don't happen by chance — they result from a culture in which security is ingrained and embodied within and by everyone.

- □ **Lead by example:** Executives should not be exempt from the security requirements that apply to the rank and file — attackers routinely take advantage of such exceptional treatment.
- □ **Hold employees, the extended workforce, and third parties to the same high standards:** Anyone who has access to any part of your IT environment should be subject to the same access controls and security policies.
- □ **Implement a comprehensive security awareness program:** This helps users understand how they can be targeted and how they are a critical line of defense against threat actors and breach attempts.
- □ **Talk about security:** The need for security should be understood by everyone as an everyday reality of doing business. Create forums where people can ask questions; designate experts who can be consulted on specific decisions; review security metrics at all-hands meetings — whatever it takes to keep security top of mind.

Consider an IR retainer with an organization that staffs ransomware negotiators

The hope is you will never need to activate this retainer or employ these professionals, but if you do, you'll be relieved that they are available.

- □ **Prioritize incident readiness.** Prepare for severe cyber attacks by creating an incident response plan, utilize incident runbooks, and reference/update preparedness materials often.
- □ **Find a partner you can trust.** A full-service incident response (IR) team should provide everything needed to stop an attack and quickly restore your organization to pre-incident business operations.
- □ **Seek an IR team with negotiation expertise.** When finding a trusted IR partner, examine the negotiation services and expertise – specifically, data regarding reduced ransoms or not paying the ransom at all.
- □ **Have insurance and legal approval.** Many cyber insurance and data privacy councils have preferred incident response providers who have familiarity with legal processes and policy requirements that ensure a collaborative engagement with any organization and third parties to address legal – and insurance-related requirements.

CONCLUSION

Adapting and evolving, together.

In this report, we've examined aggregated IR case data pertaining to ransomware, business email compromise, and intrusion incidents.

We hope the insights and recommendations herein will allow you to take a practical, prioritized, and informed approach to reducing risk and increasing resilience.

Taking a broad view of the situation, the fact that such incidents continue to occur — that is, despite massive effort and expense directed towards prevention — speaks to two important realities with which today's organizations must contend.

01

First, adversaries are committed to their 'craft,' adapting and evolving as needed to achieve their goals.

With strong financial (and sometimes political) motivations, and unencumbered by laws, certain ethical standards, or institutional planning horizons, attackers of all types show a willingness to:

- **Stick with what works:** tried-and-tested approaches including favored exploits, specific intrusion tools, and preferred strategies
- **Constantly develop new TTPs:** from low-tech methods of bypassing high-tech tripwires to the most advanced zero-day exploits — and everything in between

02

Second, preventative measures alone are insufficient. Yes, defenders must build and maintain a foundation of fundamentals and continually adapt and evolve their security posture such that, over time, those novel defenses are integrated into the new normal.

But defenders must also augment these proactive measures with:

- Reactive capabilities designed to quickly and effectively detect and respond to attacks that break through outer defenses
- Risk transfer measures, including leveraging warranties and insurance, in response to the reality that — as this report has shown — incidents do happen (even to well-prepared organizations)

It can all seem overwhelming — but you're not alone.

An entire cybersecurity community stands with you and is committed to sharing and learning, lifting and helping, and working together to withstand attacks and intrusions.

If you'd like to augment your internal capabilities with external expertise, we're ready for you to join the Pack.

How Arctic Wolf can help

The outcomes you need, the convenience you'll love.

When we speak with organizations around the world, we're often asked for three things:

01 **An effective cybersecurity solution that will provide end-to-end protection against cyber threats, that will be easy to manage, and that will integrate with the security products they've already deployed**

02 **A way to financially offset the remaining risk**

03 **Expert assistance to help evolve their security posture over time, aligned with their specific priorities and operating context**

In response, we've created the Arctic Wolf Security Operations Bundles.

These bundles provide the full suite of technology, security expertise, and risk transfer options to end your cyber risk.

Whether it's proactive security offerings like employee awareness training, vulnerability scanning, and incident readiness planning, or reactive detection, remediation, and active response capabilities to minimize the severity of an incident, the Security Operations Bundles provide full coverage across all your attack surfaces.

Best of all, some of the remaining risk may be financially transferred to Arctic Wolf through our industry-leading Security Operations Warranty. With up to $1.5 million (USD) in financial coverage and the ability to fund your cyber insurance deductible, your out-of-pocket costs after a severe cyber attack may be mitigated.

If you aren't getting the outcomes you're looking for from the solutions you have today — or if you just need some support in putting your existing investments to work — we would love to help.

For more information about Arctic Wolf, visit **arcticwolf.com**

Arctic Wolf and its employees are not licensed producers and therefore are not engaging in the sale, solicitation or negotiation of insurance and are NOT offering advice regarding insurance terms, conditions, premium rates or claims. Customers interested in purchasing Cyber Insurance coverage should consult with an appropriately licensed insurance broker.

END CYBER RISK

ARCTIC WOLF

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk.

Powered by threat telemetry spanning endpoint, network, identity, and cloud sources, the Arctic Wolf Aurora Platform ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button so customers can defend their greatest assets at the speed of data.

For more information about Arctic Wolf, visit **arcticwolf.com**.

REQUEST A DEMO