Carbon Black.

QUARTERLY
INCIDENT RESPONSE
THREAT REPORT

China, Russia & North Korea Launching Sophisticated, Espionage-Focused Cyberattacks

The world's leading incident response (IR) professionals are seeing an uptick in lateral movement, counter incident response and island-hopping attacks from motivated nation-states.

JULY 2018

Executive Summary/Highlights

Even as a steady drumbeat of headlines keeps the world's attention focused on cybercrimes, such as ransomware and cryptojacking, in the dark corners of the internet, attackers are busy refining their craft. According to the world's top incident response (IR) professionals, cyberattackers are honing their ability to remain undetected inside the enterprises they've breached, and evolving their attacks to counter defenders' response efforts.

This evolution coincides with mounting geopolitical tensions. Nation-states such as Russia, China, Iran and North Korea are actively operationalizing and supporting technologically advanced cyber militias.

Most organizations remain woefully unprepared to combat such attacks. The majority have yet to create and implement proactive incident response plans, continuing instead to lean heavily on outdated legacy antivirus and firewall tools for protection.

In an effort to gauge the current attack landscape and to quantify the latest attack trends seen by leading IR firms, **Carbon Black is introducing its Quarterly Incident Response Threat Report (QIRTR).** This report aggregates both qualitative and quantitative input from leading Carbon Black IR partners, who on average participated in one incident response engagement per day over the course of 2017. Data from this report represents insight from active breach investigations where, in most instances, some combination of people, process and legacy security technology has failed. Of note, several questions from the survey were multi-select. As a result, total figures exceed 100%.

If this report reveals anything, it's that business leaders can no longer get by thinking an attack won't happen to them. Attacks that were once reserved for sophisticated campaigns have become an **everyday reality**.

Among the Key Findings:

1. **The vast majority of cyberattacks originate from two nation-states: 81% of IR professionals say the majority of attacks come from Russia; 76% say the majority come from China.** And these foreign actors are seeking more than just financial gain or theft — **35%** of IR professionals say attackers' end goal is **espionage**.

2. **Geopolitical tension** is driving an evolution in cyberattacks against all verticals, but **78% of IR professionals** say the **financial industry** is attacked most often; **73% say healthcare organizations** and **43% say government**.

3. **Nearly 60% of attacks now involve lateral movement,** which means attackers aren't just going after one component of an organization. They're getting in, moving around and seeking more targets as they go. Of note, **100% of respondents** say they've seen **PowerShell** used for attempted lateral movement.

4. **Nearly half (46%) of incident response professionals** say they've experienced instances of **counter incident response**, another concerning sign that attackers have become increasingly sophisticated and are initiating longer-term campaigns — as well as a clear signal that incident response must get stealthier.

5. **More than a third (36%) of today's attackers** now use the victim primarily for **island hopping**. In these campaigns, attackers first target an organization's affiliates, often smaller companies with immature security postures. This means that not only is your data at risk, but so is the data at every point in your supply chain, including that of your customers and partners.

If this report reveals anything, it's that business leaders can no longer get by thinking an attack won't happen to **them**. Attacks that were once reserved for sophisticated campaigns have become an everyday reality. Attackers are using increasingly sophisticated techniques and can easily evade standard defenses, our IR partners noted. Perhaps most importantly, the consequences of geopolitical conflict can have a tangible impact on global organizations and our connected way of life.

THE TOP 3 INDUSTRIES MOST OFTEN TARGETED BY CYBERATTACKS

Financial	78%
Healthcare	73%
Government	43%
Retail	32%
Manufacturing	22%
Food and Beverage	14%
Oil and Gas	11%
Professional Services	8%
Media and Entertainment	3%
Other	16%

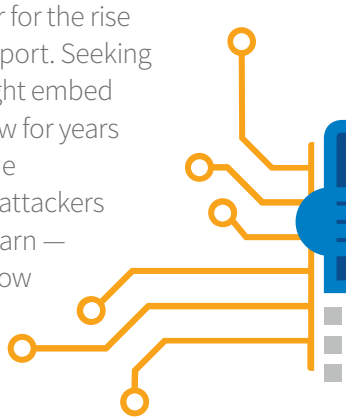
Carbon Black.

Fraught Geopolitical Tensions Play out in Cyberspace

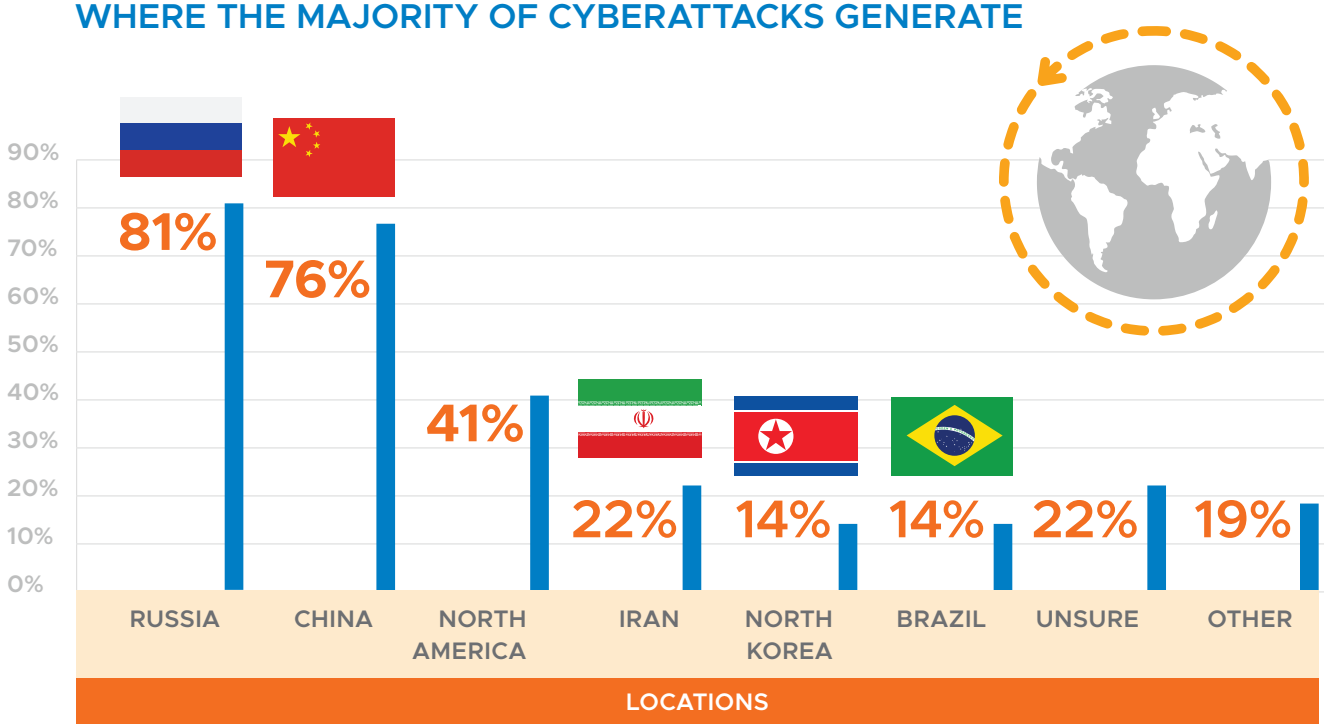
Geopolitical tension is a historical constant, but today's conflicts are increasingly playing out in cyberspace, where subversive acts can be devastating and nearly impossible to prosecute. The result is an evolution in cyberattacks across all verticals, with the **financial industry** the most frequent target **(78% of respondents say as much)** followed by **healthcare (73%)** and **government (43%)**.

Some foreign actors, such as China, are continuing to seek competitive economic advantage, calculating, for instance, that it might be easier to steal IP from an American defense contractor than develop it themselves. Others have political motives, as seen in Russia's hack of the Democratic National Committee during the 2016 U.S. election and the recent cyber campaign against the U.S. energy sector. As economic pressures and political tensions grow, more and more nation-states are finding it politically and financially advantageous to leverage cyber militias in sophisticated attacks. It is much less expensive (and stealthier) to launch a cyberattack than it is to launch a nuclear weapon.

These attackers have served as a harbinger for the rise of long-term campaigns depicted in this report. Seeking to avoid detection, nation-state actors might embed themselves on foreign networks and lay low for years before taking overt action. According to one IR professional interviewed for this report, attackers also linger simply because "they want to learn — learn the network, where the data is and how they can get it without setting off alarms."

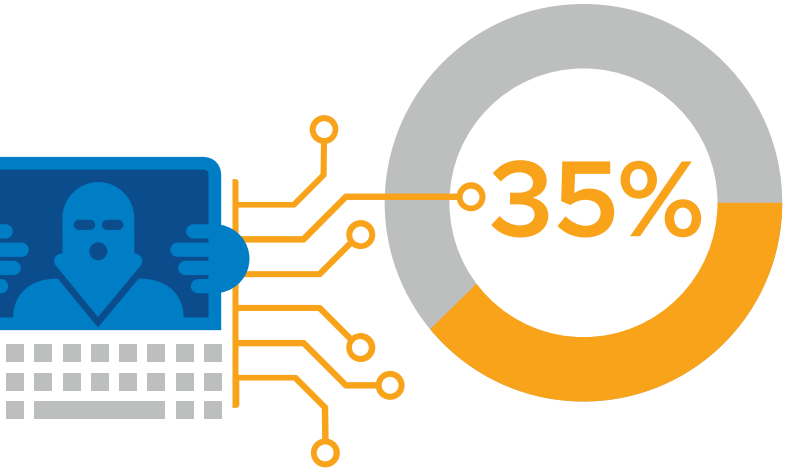


WHERE THE MAJORITY OF CYBERATTACKS GENERATE



Carbon Black.

35% OF RESPONDENTS SAY ATTACKERS' END GOAL IS ESPIONAGE



It's fitting, then, that **more than a third of all respondents (35%) see espionage as a primary motive for attackers.** They also frequently cited **business disruption** and **blackmail**, at **19%** and **14%** respectively.

Moreover, nation-state actors introduce techniques and tools that enable more rudimentary attackers to take increasingly high-level actions. For example, speaking about the series of powerful Petya cyberattacks waged against Ukraine in 2017, one IR professional says, "A year ago it was top-shelf Russian malware, and now some joker doing cryptocurrency mining is using the same thing…mechanisms out there are tough to contain and malware spreads fast."

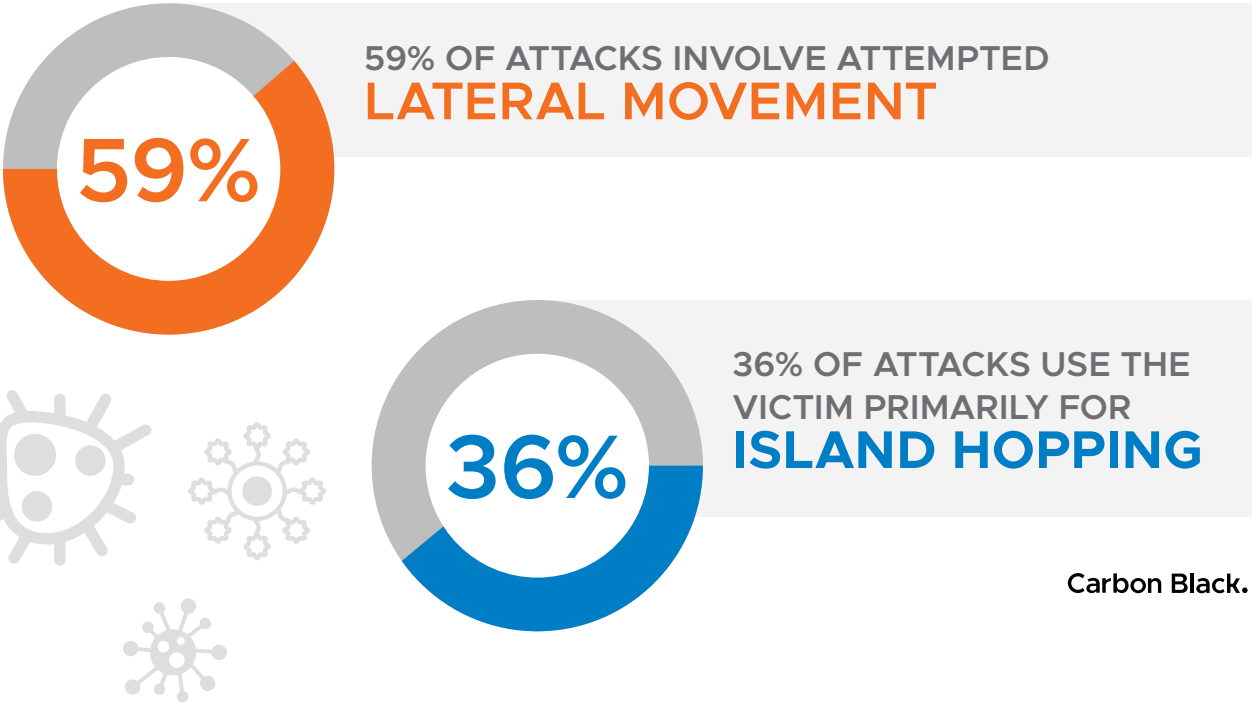
An Evolution of Cyberattacks — From Grab-and-Go Breaches to Long-Term Campaigns

The data in this report reveals that today's cyberattacks manifest as increasingly complex, long-term campaigns. Employing high-level tools and techniques, attackers set out to take over an organization's infrastructure — allowing them to move throughout the network.

Note the high percentage **(59%) of respondents who say attacks nowadays involve lateral movement within a network.** And a growing number of hackers won't stop at a single network — they're after your clients' partner and customer infrastructure as well. A full **36% of our respondents say they see attacks where the victim was primarily used for island hopping.**

This shift reflects an evolution in the way businesses use and handle data. On the one hand, more and more data is consolidated and shared among organizations. At the same time, this data is increasingly decentralized across networks due to cloud computing — making it harder for attackers to quickly find everything they want. "Our customers' IT teams don't even know where all their assets are," one IR professional says. "So it makes sense that attackers need more time to figure it out."

And as attacks become increasingly protracted and complex, eluding detection becomes a top priority for hackers: nearly half of respondents (46%) report seeing instances of counter incident response.



"Our customers' IT teams don't even know where all their assets are. So it makes sense that attackers need more time to figure it out." — **IR professional**

CASE STUDY: A Cryptomining Attack — With an Assist From Advanced Malware Techniques

One day in early summer, a healthcare company noticed something troubling: An abnormally high volume of network traffic was inflicting downtime at several store locations. At first they thought it was an external attack — like a distributed denial of service — and legacy antivirus was unable to identify the threat. The finding from their ISP was even more troubling: the traffic was coming from the inside.

At this point they called in Kroll, which immediately installed Cb Response to gain visibility into the network. They saw that infected machines were causing a "traffic jam" because they were continuously scanning to find others to infect. Kroll also identified malware known as WannaMine trying to enlist as much computing power as possible to mine cryptocurrency.

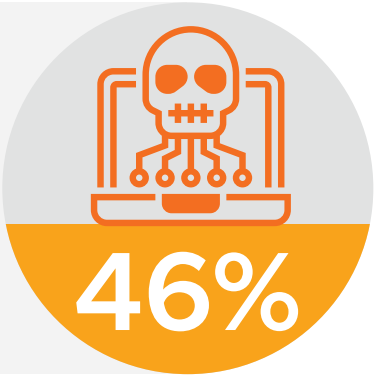
Kroll has a long history working with these sorts of attacks. It used Carbon Black to run relevant queries, cross-check systems for suspicious behaviors and search running processes for cryptomining algorithms. Rather than imaging all 500 systems in the network, it could prioritize — using Carbon Black to identify the systems most likely to have permitted the malware's initial entry. The data told Kroll the attacker had embedded code within PowerShell commands to obtain credentials using a variant of Mimikatz, run the miner and then spread itself via the WMI and SMB protocols. Two persistence mechanisms were also used: a WMI event consumer and scheduled tasks. The attackers might have been low-level cryptominers, but they were using high-level malware techniques made available, in part, by nation-state actors who employ standard Windows tools and protocols to evade traditional security defenses.

To remediate and recover from this attack, Kroll used Cb Live Response to surgically terminate the malicious PowerShell processes and remove the persistence mechanisms. Scripting against the Cb Live Response API meant that Kroll could do this across all affected systems quickly. Within days, as the Carbon Black deployment was completed, Kroll's IR team restored network performance. The traffic let up and the coast was clear for business to return to normal.

Kroll®

46% OF IR PROFESSIONALS SEE

COUNTER INCIDENT RESPONSE DURING IR ENGAGEMENTS



64% OF IR PROFESSIONALS SEE INSTANCES OF

SECONDARY C2

BEING USED ON A SLEEP CYCLE DURING IR ENGAGEMENTS

"Attackers are living off the land. They're not bringing tools in with them, but using Windows against Windows. It makes them harder to find." — **IR professional**

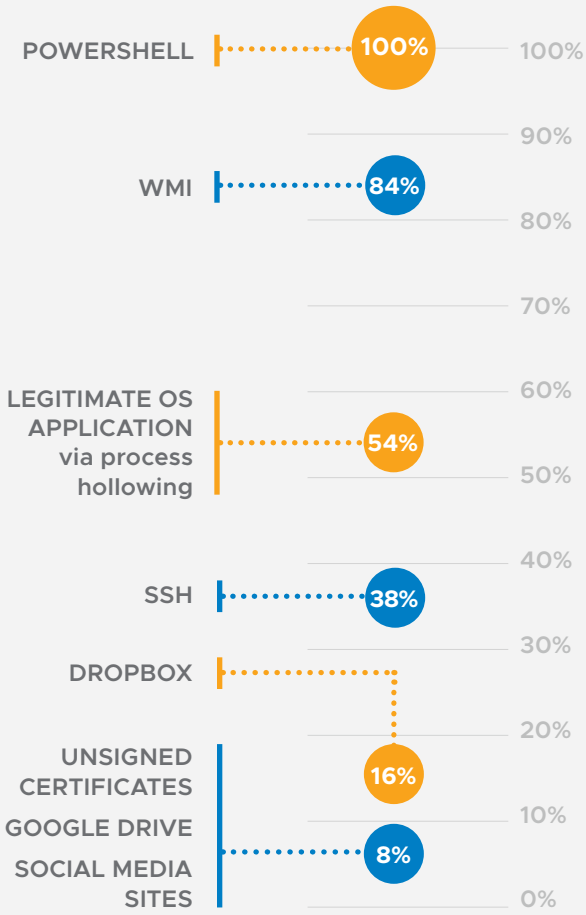
Carbon Black.

What's more, attackers are adapting to commonly employed security systems. **Nearly two-thirds (64%) of respondents, for example, see instances of secondary C2 used on a sleep cycle during their IR engagements,** suggesting that network-based protections, which are regularly deployed to shut off hackers' secret passages in your network (C2), have ostensibly been rendered useless; attackers are using a second C2 that wakes up only after the initial one goes down.

PowerShell and WMI Remain Tools of Choice for Cyberattacks

We've long known that **PowerShell** has been abused, but it is still significant that **100% of respondents say they believe the tool most often helps facilitate lateral movements, followed by WMI at 84%.** As one IR professional puts it, "Attackers are living off the land. They're not bringing tools in with them, but using Windows against Windows. It makes them harder to find."

WHAT DUAL-PURPOSE TOOLS FACILITATE LATERAL MOVEMENT FOR ATTACKERS?



Carbon Black.

100% of respondents chose PowerShell as the tool that facilitates lateral movements for attackers, with WMI as the second choice. Some other tools stated by respondents include PsExec.exe, BITSAdmin.exe and Remcom.

That **54% of respondents also see legitimate OS applications being used** (via process hollowing) points to the growing severity of such attacks — it can be especially difficult to purge bad actors when they have found a way into the very foundation of your network. Of note, too, is that **16% of respondents see Dropbox as a primary tool for helping facilitate lateral movements,** demonstrating hackers' growing familiarity with cloud services.

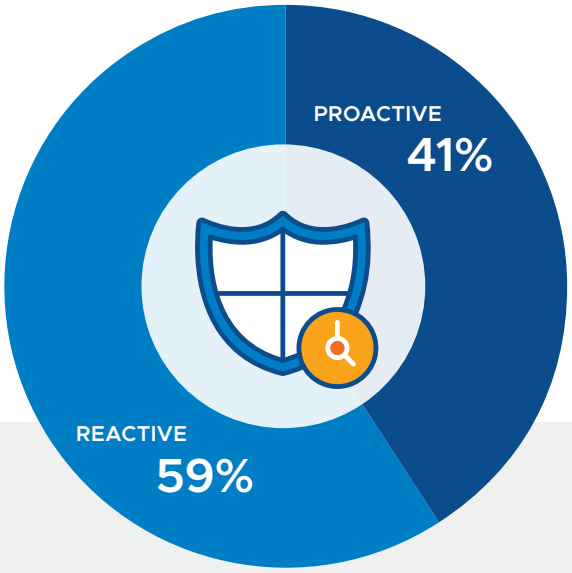
The gravity of today's cyberattacks can't be understated. **When asked how often targeted victims experience destructive/integrity attacks, respondents say they occur at least 10% of the time.** And yet the vast majority of organizations remain unprepared. **Fifty-nine percent of respondents say the organizations they serve take a reactive, rather than a proactive, stance toward incident response.**

"Most cases we see [that organizations] don't have an IR plan in place," one IR professional says. Detection capabilities is a major gap — **nearly 70% of respondents say lack of visibility is a top barrier to effective incident response** (a shortage of skilled security experts and inaccurate/decentralized log keeping are other major obstacles). "Most organizations rely on their IT department and on [legacy] antivirus and a firewall [for IR]," one IR professionals says. "They are easily dismantled; firewalls are useless against inside-out attacks, and unequipped IT departments can often do more harm than good."

At the end of the day, some say, the continual lack of preparation in the face of such threats comes down to human nature. "The human mind is not great at predicting and investing in nebulous threats that haven't happened to you," says one IR professional. "If you haven't been hit, or if a peer hasn't been hit, nothing will get done. Most companies wait until something bad has happened."

59% OF IR PROFESSIONALS SAY ORGANIZATIONS THEY WORK WITH FOLLOW A REACTIVE APPROACH TO INCIDENT RESPONSE

Carbon Black.



"If you haven't been hit, or if a peer hasn't been hit, nothing will get done. Most companies wait until something bad has happened." — IR professional

CASE STUDY: Hunting an Attacker Who Knows How to Cover His Tracks

There are certain seminal experiences you'll remember all your life — your first kiss, your college graduation, the smell of your favorite home-cooked meal — and then hundreds of mini-experiences that helped you reach each milestone that in short order disappeared from view.

The memories you carry with you forever? That is similar to what computers save to disk. The other stuff? That's similar to (ironically enough) system memory. Attackers used to execute malicious code on disk, where legacy antivirus could better detect it. Today, as Black Cipher's IR team saw firsthand at a large real estate and investment firm, cybercriminals have become sophisticated enough to carry out attacks through memory. As memory fades, the attackers' tracks are covered, which makes detection — and ultimately remediation — a true challenge.

The malware, in this case, came in through a malicious Microsoft Word document labeled as an invoice. When someone inside the organization opened it, an attack was launched that ran a macro that called on the command prompt, which then called on PowerShell, which went to a malware distribution server, pulled down a malicious executable, ran it and then deleted it. The malware called back to a command-and-control server which resulted in the attacker establishing a covert tunnel to the inside of the network. This tunnel opened the door for further activities such as data exfiltration, logging of keystrokes, credential theft and lateral movement.

This breach would have been virtually impossible to detect had it not been for Carbon Black's Advanced Threats feed combined with Cb Response's ability to create custom watchlists, which gave Black Cipher the network visibility it needed to identify the entry point and terminate the attacker's connection. What's more, the tool allowed the IR team to remotely extract system memory to understand the nature of the threat (e.g., are they taking screenshots? Pulling documents?). This was especially crucial because the client fell under NYDFS 500 compliance and needed to quickly know whether or not to report.

Within two hours, the IR team had the attacker out of the system and was able to provide the answers their client needed in order to determine their compliance reporting requirements. The speed and efficiency of Black Cipher's response were abetted not only by Carbon Black but by their client's own proactive IR plan, which, in this case, immediately initiated credential change and other protocols that softened the blow of the attack.

Incident response like this? Definitely worth remembering.

Taking a Proactive Approach to Incident Response: Six Tips From IR Pros

A proactive approach to IR doesn't necessarily require a massive investment — it's just as important to have strong communication, basic pre-planning and simple (yet consistent) protective measures. Here's what IR professionals say are the most important things to know:

1. HAVE AN IR PLAN IN PLACE. In the **"fog of war,"** as one IR professional describes incident response, "if you're not trained to properly respond, people panic and make mistakes, they lose evidence. So many things can go wrong if you don't have a well-laid-out plan." But where to begin? It starts with tabletop exercises. **"You sit down with the company and run scenarios. Say a phishing attack comes in — where do you go from there? And after that, then what? The series of questions causes people to think critically about these things,"** one IR professional noted. From there, you should be able to develop a plan outlining protocols and role responsibilities for each stakeholder at your organization.

2. COMMUNICATE AND NOTIFY. Efficiently managing through an attack means telling the right people in your organization about the right things at the right times. This could mean everyone from your board of directors to your in-house counsel to your customer service representatives. The key is having distribution lists in place, as well as proper messaging for various stakeholders.

3. KNOW YOUR LEGAL REQUIREMENTS. All 50 states now have their own reporting requirements for certain cybersecurity incidents. You need to be clear about what and when you need to report and, if so, which questions you'll have to answer about the incident. In today's complex compliance environment, it's crucial that organizations think through every last possibility. **"When an email inbox gets hit at, for instance, a real estate company,"** one IR professional says, **"that attacker could now have access to loan applications from different states. All those states may need to be notified."**

4. VISIBILITY IS KEY. Attackers will breach your defenses — that's nearly inevitable — and they're getting better at covering their tracks. At the same time, as networks become more and more complex, an organization's assets can be hard to map. Thus it should come as no surprise that **68% of respondents report lack of visibility as a primary barrier to effective incident response.**

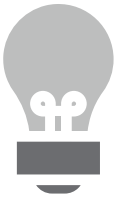
It is imperative to improve situational awareness. On the one hand, remedying this problem entails, as one IR professional suggests, **"breaking down your network into users, host and processes,"** and profiling each one with the help of an EDR tool.

Just as important, though, is data centralization: a central SIEM that has all your specific event logs and login IDs. **"Most of the time you want to be proactive,"** the IR professional adds. **"The best thing to do is learn about the data you already have."**

5. HUNT QUIETLY. Once you detect an attack, don't immediately rock the boat — the substantial amount of counter incident response noted by respondents shows that attackers can cut your legs out from under you if you make your presence known too overtly. **"We're hunting too loudly,"** says Tom Kellermann, chief cybersecurity officer at Carbon Black. **"It's like if someone breaks into your house and you call out, 'I have a gun and I'm calling the cops!' You're making assumptions about the attacker: that there's a single adversary, that they're scared of you, that they won't burn the house down on the way out the door. Most attackers have a demigod complex because they know they won't be prosecuted — so they may choose to be punitive."** Deciding when to reveal oneself is critical.

6. REGULAR CHECKUPS + MULTI-FACTOR AUTHENTICATION. Periodic risk and vulnerability assessments can go a long way. And single-factor authentication is a massive liability. As one IR professional says, **"People who have multi-factor authentication and conduct regular vulnerability scans on their infrastructure tend not to call us."**

68% of IR professionals say lack of visibility is a primary barrier to effective incident response



CASE STUDY: No More IR Busy Work

What IR teams want to spend time doing: finding the bad guys ASAP and saving customers money.

What IR teams really don't want to spend time doing: administrative overhead.

From discovery to data acquisition to remediation, IR teams might spend hours of their precious time doing tedious labor — for instance, going in and grabbing an organization's relevant forensic artifacts (such as event logs) one by one.

This would have been a major obstacle for Rapid7's IR team when dealing, of late, with an international law firm whose servers and workstations had been hit by SamSam ransomware. But by working with Carbon Black's open API, Rapid7 developed tools to automate several of these time-consuming processes.

In this case, Rapid7 used an in-house tool, Cb Deploy, to send a script throughout the network to find systems containing a certain XML file related to the malware — and they did so all at once, rather than pushing it out to one system at a time. They then used another tool, Cb Mass Acquire, to collect all the relevant artifacts for the infected systems to find the root cause. Rather than doing this manually — and then, only when the systems are online — their tool can acquire from multiple systems at once while automatically re-queueing jobs for systems that are offline at the time of job scheduling. Finally, Rapid7 used their Cb Timeliner tool to create, in seconds, a master timeline of what went down, before guiding the client through remediation.

These are just a few examples of how, working with Carbon Black's developer relations team, Rapid7 has cured common IR headaches with innovative solutions.

RAPID7

Conclusion

The high numbers of counter incident response, lateral-movement attacks and island hopping all underscore the evolving nature of cyberattacks: from grab-and-go breaches to complex long-term campaigns. Geopolitical tensions show no signs of abating. And so the developments described in this report, and the insights that help make sense of them, represent the early skirmishes in what will certainly be a long, difficult and perpetually evolving battle in cyberspace.

The data points outlined in this report should serve as a signal fire for business leaders whose organizations remain unprepared and purely reactive in the face of today's imminent cyber threats. To combat the attacks of tomorrow, leadership must take action today, with a focus on heightened visibility and quick detection across networks.

For despite significant investment in cybersecurity, the vulnerabilities continue to proliferate, giving bad actors more and more opportunities to strike with relative ease. Part of this is about technology of course, but as one IR professional puts it, "It's also a human problem."

While this is certainly cause for concern, it should also be a cause for hope: If we're part of the problem, we also have the power to be part of the solution.

To combat the attacks of tomorrow, leadership must take action today, with a focus on quick detection and heightened visibility across networks.

Methodology

Carbon Black conducted an online survey about trends in incident response in June 2018. The results from this report comprise responses from 37 leading IR organizations, all partners of Carbon Black. Percentages in certain questions exceed 100% because respondents were asked to check all that apply. Due to rounding, percentages used in all questions may not add up to 100%.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 4,000 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform — the Cb Predictive Security Cloud — Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus.

Part of this is about technology of course, but as one IR professional puts it, "It's also a human problem."

While this is certainly cause for concern, it should also be a cause for hope: If we're part of the problem, we also have the power to be part of the solution.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com