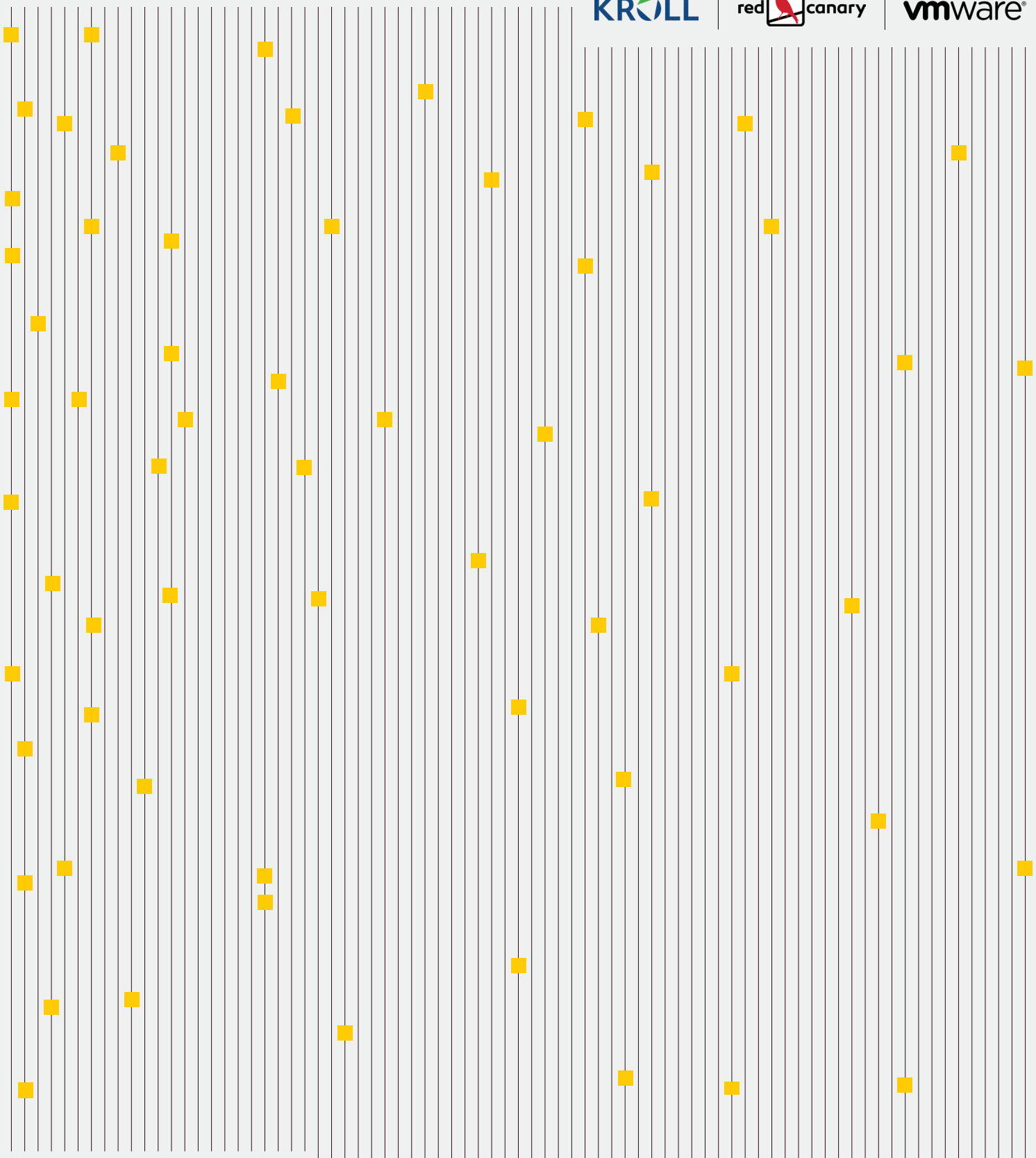


The state of incident response 2021: It’s time for a confidence boost

Introduction

There's a need now more than ever for security organizations to implement a structured, detailed, and well-practiced incident response plan. As the Navy SEALs training philosophy goes, "slow is smooth and smooth is fast"—a mantra that can, and arguably should, be adopted by all security teams. In incident response, speed comes from being prepared to methodically and efficiently shut down adversaries in cases where they manage to get past defenses.

The COVID-19 pandemic has brought to light inefficiencies or a lack of preparedness within security teams. All at once, security teams found themselves dealing with an influx of personal devices on the corporate network, greatly reducing endpoint visibility and expanding the potential attack surface, at the same time that attack vectors were, and continue to be, on the rise.

The pandemic also provided security teams with an opportunity to evaluate their state of preparedness as well as the effectiveness of their incident response policies to make refinements going forward. To better understand the state of incident response today and identify areas for improvement, **Kroll**, **Red Canary**, and **VMware** partnered with Wakefield Research to survey 500 security and risk leaders at large organizations—those with more than $500 million in revenue—on matters related to their cybersecurity programs, specifically threat detection and incident response.

In this report, we'll dive into the survey results; present insights and analysis from cybersecurity experts; and reveal real-world concerns from organizations. Finally, we'll recommend actionable steps organizations can take to shore up their incident response plans and stroll into this digitally transformed world with newfound confidence.

> "Reputational damage should become the driver, as cybercriminals colonize corporate networks. In the absence of vigilant cybersecurity, your digital transformation will be commandeered."

Tom Kellermann
Head of
Cybersecurity Strategy
VMWARE

Key takeaways

No organization is immune to attack

The vast majority (93%) of organizations suffered a compromise of data over the past 12 months, and most security leaders (82%) believe their organization remains vulnerable to a cyber attack.

Deficiencies in incident response persist

Nearly half of organizations (49%) are not equipped to meet cybersecurity challenges, while others (54%) are wasting valuable time investigating low-level alerts and slowing down the incident response process.

Lack of best practices is putting defenses at risk

While most organizations are following best practices, the research shows there is room for improvement. As many as two in five organizations are failing to perform compliance audits of partners handling sensitive data (41%) or are lacking an employee security awareness program (37%).

Collaboration between legal and infosec is inadequate

Almost half (47%) of security leaders say their teams lack clarity about when to engage legal counsel about a potential incident. Further, at least two in five organizations are ill-equipped to respond to the full legal requirements of handling a security incident. Augmenting these struggles, 39% of organizations are leaving themselves exposed by not having a cyber liability insurance policy to cover cyber incidents and data breaches.

49%

Nearly half of organizations lack adequate tools (including staff and expertise) to detect or respond to cyber threats.

Third-party security providers are integral to organizations' incident response processes

The majority of security leaders believe that third-party providers can help the most with speeding up containment and response to threats (55%), augmenting in-house expertise (53%), and increasing automation of processes (50%).

Organizations are combating intensifying threats

All aspects of an organization can be impacted by an attack, security leaders say. Their concerns cover quite a range, some more tangible and easier to spot than others.

SECURITY LEADERS ARE CONCERNED ABOUT AN ARRAY OF NEGATIVE IMPACTS FROM CYBER ATTACKS

"American cyberspace is reeling from a cyber insurgency stoked by the pax mafiosa between the cybercrime cartels and rogue regimes. Counter incident response is now occurring 63% of the time and destructive attacks have surged by 118%. 2021 is defined by a renaissance in exploit development and a strategic embrace of island-hopping as the preferred modus operandi."

Tom Kellermann
Head of
Cybersecurity Strategy
VMWARE

The threats are real and have been felt by nearly all organizations. In just the past year, 93% of organizations have suffered at least one incident that led to a compromise of data, and nearly half (49%) of these organizations had at least four such incidents.

While security leaders are clearly aware of the negative impacts that can come from not having the right security controls in place, there remain gaps that are leaving organizations susceptible to further serious incidents: Two-thirds (66%) of security leaders say that their organization is vulnerable to a cyber attack that could disrupt business or lead to a data breach.

Of note, regarding vulnerability, security leaders generally positioned their organizations more favorably against their competitors—compared to the two-thirds of respondents self-identifying as vulnerable, 82% said the average organization in their industry is vulnerable to attack.

FOOD FOR THOUGHT:

Our survey suggests a certain level of bias in security leaders' perceptions of their own organizations' security posture, which could provide a false sense of security and potentially cause critical problems or gaps in coverage to go overlooked.

Further, companies with less than $1 billion revenue (71%) are more concerned about data compromises and loss of sensitive information than companies with more that $1 billion revenue (56%). If revenue is an indicator of business maturity, this could suggest that more mature organizations have at their disposal more resources such as legal counsel to help share the burden of responding to a breach and cushion potential fallout.

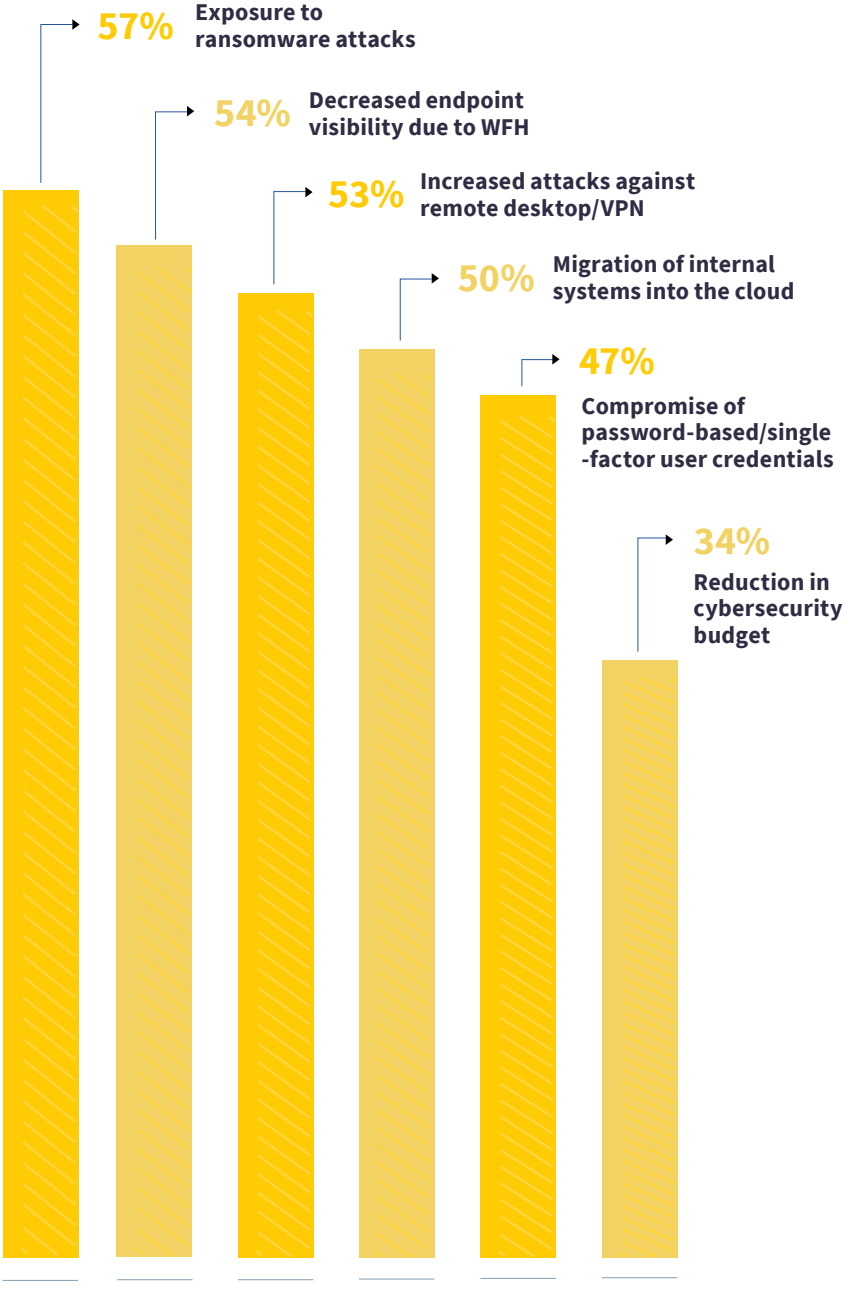
"Many organizations prepare by conducting a tabletop exercise with a handful of stakeholders, but when faced with a real incident their front-line teams lack clarity to properly classify and declare an incident response. Organizations need to develop and enforce clear-cut escalation frameworks to avoid costly delays."

Stacy Scott
Managing Director,
Cyber Risk
KROLL

Identifying threats

Few business functions had to adjust to the COVID-19 crisis as quickly as security teams. When organizations made the shift to a work-from-home (WFH) model, not only did security teams have to work very quickly to establish secure connections, but they also had to be on the lookout for threats targeting remote workers.

SECURITY LEADERS CITE INCREASING SECURITY CONCERNS OVER THE PAST YEAR



“

Over the course of 2020, as organizations shifted already overburdened staff to build capacity to support remote working, threat actors aggressively exploited weaknesses exposed in the transition.”

Marc Brawner
Global Head of Managed Security Services
KROLL

The new risks are diverse and substantial. Exposure to ransomware attacks has been a high-profile threat for some time and has continued to grow in prominence over the last year, according to 57% of security leaders. Prior to the remote work surge brought on by COVID-19, tools like network-based threat detection and web proxy filters were traditionally implemented on premises at a corporate location. Now, security teams are staring down a proliferation of employee-owned endpoints that are accessing the corporate network and causing visibility challenges. The reduction in endpoint visibility due to working from home has become an increased concern for most security leaders (54%). Elsewhere, increased attacks against remote desktop services (53%) and the migration of internal systems to the cloud (50%) have also become greater threats.

Nearly half (47%) of security leaders pointed to identity compromise through password-based/single-factor user credentials as a growing area of concern for their organization. However, this has long been a commonly used attack vector, made attractive to adversaries simply because gaining access to a system as an authorized user is much more efficient than attempting to target the built-in security of operating systems. We also commonly see a remote desktop or other service exposed to the internet with single-factor authentication serve as the initial entry point for an adversary, then leading to lateral movement and ultimately ransomware.

FOOD FOR THOUGHT:

The fact that such a large portion of the respondent base sees identity compromise through password-based/single-factor user credentials as a growing area of concern shows that this pain point has not been adequately addressed yet. Strong identity protection, including multi-factor authentication, remains a vital tool in slowing adversaries.

“

There is nothing more effective at slowing down or stopping an adversary than strong identity protection, including multi-factor authentication. It doesn’t prevent all attacks, but it would prevent an overwhelming majority.”

Keith McCammon
Chief Security Officer
& Co-founder
RED CANARY

Internal obstacles hindering security

While security leaders attempt to deal with heightened external risks, they are also facing substantial internal obstacles. For example, despite escalating threats, 45% of organizations surveyed said that their security spending will stay the same or decrease over the next 12 months. Resources continue to be a challenge, and these organizations will be required to do more to respond to the changing threat landscape with existing resources.

POSITIVE +

55%

Increase cybersecurity spending over next year

52%

Regular security readiness with leadership

NEGATIVE -

47%

Security processes seen as impediment

42%

Lack of organization-wide support

42%

Information security program meets only minimum requirements

41%

Leadership doesn't understand initiatives

Security leaders also say they lack resources to properly address threats, so in some cases, the decision by an organization to not increase their spending will only exacerbate glaring weaknesses.

49%

About half of security leaders say their organization lacks adequate tools to prevent, detect, or respond to threats

46%

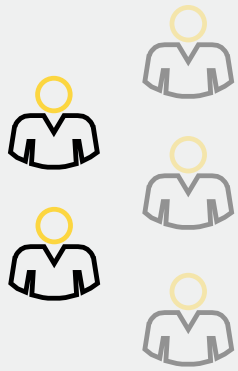
More than four in 10 say they do not have adequate staffing on their security team

44%

More than four in 10 say the staff they do have lack adequate expertise

Difficulty adhering to best practices

While many security leaders are following best practices, there is ample room for improvement in this area.

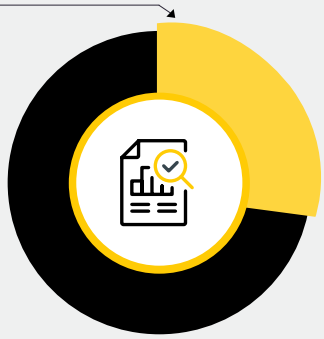


41%

As many as two in five security leaders are failing to implement compliance audits of partners and vendors who handle sensitive data, making the organization more vulnerable to third-party data breaches.

29%

Nearly one-third don't have a formalized information security strategy at all.



If a large percentage of security programs are not auditing third-party vendors for compliance, they're also likely not auditing them for security concepts such as secure development lifecycle. This could be a critical error because if an adversary pulls off a software supply chain attack on one of your third-party vendors, then you and all of their other customers are at risk—and likely the intended targets.

Introducing best practices and formal strategies won't automatically make an organization more secure, but it will provide a clear structure, enabling easier measurement of security processes' effectiveness.

TIP

Ahead of an incident, it's important to develop an information security program that helps build a defensible narrative, including statements like:

"We have performed a threat-based assessment focused on the type of data we store and transact."

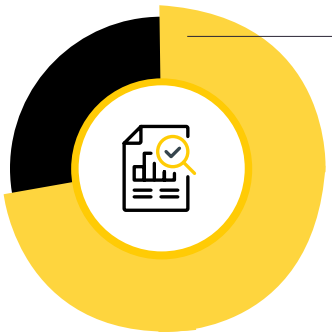
"We've taken reasonable measures to protect our data from the threats that are most prevalent to our type of business."

"If an attacker does get into our network, they would have to take extraordinary measures to bypass our security."

Andrew Beckett
Cyber Risk Practice Leader, EMEA
KROLL

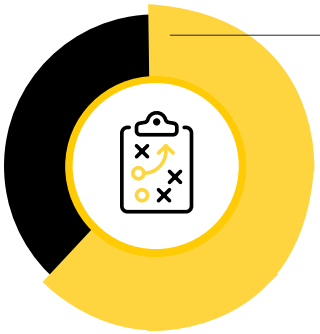
Room for progress

Rate of adoption for best practices remains low:



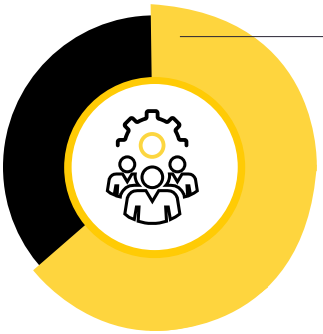
71%

Formalized information security strategy



64%

Structured incident response process

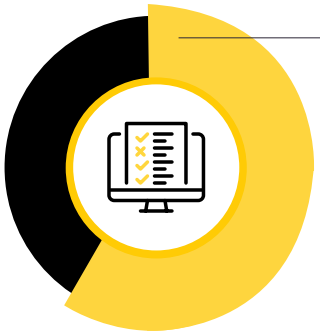


63%

Employee security awareness program

63%

Adherence to cybersecurity framework



59%

Compliance audits of partners & vendors

Incident response can be overwhelming

Many organizations are wasting valuable resources on inefficient processes, with the majority (54%) of security teams spending too much time investigating low-level security alerts. It's no surprise that security teams are pressed for time when most (70%) are bombarded with 100 or more cybersecurity threat alerts every day. Some of the most exposed organizations are also inundated with alerts: 25% of organizations that had more than three data compromises in the last 12 months are receiving more than 500 alerts a day. Many of the alerts are either innocuous or not examined at all, as most (79%) security teams at all organizations are investigating up to 20 threat events daily.

Weaknesses are evident elsewhere in the process. Only 8% of security leaders are fully confident that their organization could identify the root cause of an attack. The inability to determine the root cause can make it difficult to track threat movements and could hamper detection of what malicious activity is occuring, by whom, and in what network segments.

8%

of security leaders are fully confident that their organization could identify the root cause of an attack.

70%

of organizations are bombarded with over 100 cyber threat alerts every day.

Responding to incidents

It's imperative that processes are in place enabling triage of potential threat activity—but this requires resources to accurately sift through incoming information. It appears many security teams are lacking in this space. After the initial compromise has occurred, nearly half (46%) of organizations are typically unable to contain a threat in less than an hour. Notably, nearly a quarter (23%) of organizations that have had more than three data compromises in the past year take at least 12 hours to contain a threat.

In the worst-case scenario, an organization will suffer an attack so debilitating that operations will go down. All organizations surveyed have a disaster recovery plan, but most plans (51%) take at least one full day to recover from downtime, costing the company precious time before operations are restored. Sustained downtime can have wide-ranging negative impacts on an organization, including wasted resources, loss of business, and damage to reputation.

Given the importance of incident response, testing the process should be of the utmost importance. Security leaders are turning to a variety of methods for assessment, but many are overlooking vital practices. Less than three in five conduct incident response exercises on a regular basis (57%), update their process based on frameworks such as NIST and MITRE ATT&CK (59%), or measure changes in performance based on the response to actual incidents (57%). Even organizations that have suffered the most are neglecting key procedures — only 51% of organizations that suffered three or more data compromises over the past 12 months regularly conduct incident response exercises.

> "It's imperative to quickly identify threats during an incident and triage what's critical and what's not. This is where endpoint protection capabilities like Enterprise EDR and audit & remediation can go a long way, especially when data is correlated with the rest of your security stack."

Justin Scarpaci
Partner Solutions Architect
VMWARE

TIME FROM INITIAL COMPROMISE TO CONTAINMENT OF A THREAT

For 54%

Containment takes under an hour

For 33%

Containment takes one to 12 hours

For 13%

Containment takes 12 hours or more

Legal remains a blind spot

Since breaches can damage a company's business and create financial and legal risks, organizations must have legal participation early on. But the involvement of legal stakeholders remains a grey area for many organizations. Almost half (47%) of security leaders say their teams lack clarity about when to engage legal counsel about a potential incident.

An organization simply cannot mature without a strong incident response plan. Key to fortifying that plan is rehearsing and practicing it, running multiple scenarios to ensure that the team is prepared to take into account a variety of factors in case they have to put the plan into action.

Make legal the quarterback of incident response

LEGAL ASPECTS OF CYBERSECURITY IN AN ORGANIZATION

"Incident response is a multi-layered process, and the most important aspect of the process is a well-defined plan that includes whom to involve, when to involve them, and how. The uncertainty about engaging legal counsel speaks to a low level of maturity in incident planning overall."

Keith McCammon
Chief Security Officer
& Co-founder
RED CANARY

At least two in five organizations are ill-equipped to respond to the full legal requirements of handling an incident. These shortcomings range from teams not being fully prepared to preserve evidence for potential litigation (46%), to issues clearly defining a communication process (43%). Many are missing a clearly defined process to communicate with regulatory agencies (43%) and lack readiness to notify the public and/or its customers in the event of a security breach (43%).

The complexity of data breach and cyber incident disclosures is magnified when organizations operate across multiple jurisdictions, each with different disclosure requirements and timelines. As a recent example, a regional telecommunications company that experienced an incident received inquiries from the FCC, the FTC, and multiple state attorneys general. In another scenario, a hospitality industry business that experienced an incident received inquiries from several U.S. state and federal agencies, as well as from data privacy regulators in Italy, the UK, and Australia.

Challenges in acquiring data

Security teams' inability to fully preserve evidence extends across many forms of data. When investigating an incident, significant shares of organizations find it difficult to acquire cloud-based services logs/data (46%), threat attribution and threat actor intelligence (43%), and technical indicators of compromise (43%). The results highlight that investigative expertise alone is not sufficient if organizations are unable to obtain the relevant data.

Demystifying cyber insurance

Another potentially devastating area that organizations are overlooking is insurance. General liability insurance will typically do little to protect organizations in the event of a cyber attack. The unprotected losses can be disastrous, including stolen money or ransomware payouts, but also spreading to related costs for forensic specialists, regulatory charges, and liability.

Despite these consequences, nearly two in five (39%) organizations do not have a cyber liability insurance policy. And the organizations most vulnerable to attack are least protected: Over half (51%) of organizations that had more than three data compromises in the past 12 months do not currently have a cyber liability insurance policy.

> "Security and risk leaders need to understand the specific risks that they are looking to transfer through cyber insurance and focus on a policy that will provide that level of coverage. That might include provisions for digital forensics, data recovery, business restoration, and replacement hardware if [the] original is encrypted and there are no decryption keys available."

Jason Smolanoff
Global Cyber Risk Practice Leader
KROLL

The role of external partners in incident response

External security partners already play a significant role in the incident response process, but there is room for them to do more heavy lifting. More than three quarters (76%) of organizations use third parties as part of their incident response process. Sixty-seven percent (67%) use a combination of in-house and third-party incident response, while 9% rely on third-party incident response only. It's clear that while organizations are leveraging these external vendors, they can use their expertise further to help alleviate some of their largest incident response pain points.

Security leaders readily acknowledge that their incident response needs strengthening in various areas. Organizations want to improve the time taken to contain and remediate threats (55%), increase the automation of their incident response (55%), and reduce the time needed to respond to threats (51%). Notably, the majority (51%) of security leaders who work in corporate counsel also want to improve their breach notification readiness. Security leaders know that increased automation can help, with nearly all of them planning to automate more of their incident response process over the next year.

Despite organizations' well-intentioned plans to automate their processes, security teams are lacking the resources to execute on the strategies—showing that more assistance is needed.

> "Gone are the days of automation benefits only being realized by technical staff. There are significant efficiencies and cost savings to be gained that will benefit the entire organization."
>
> **Eric Groce**
> Incident Response Manager
> **RED CANARY**

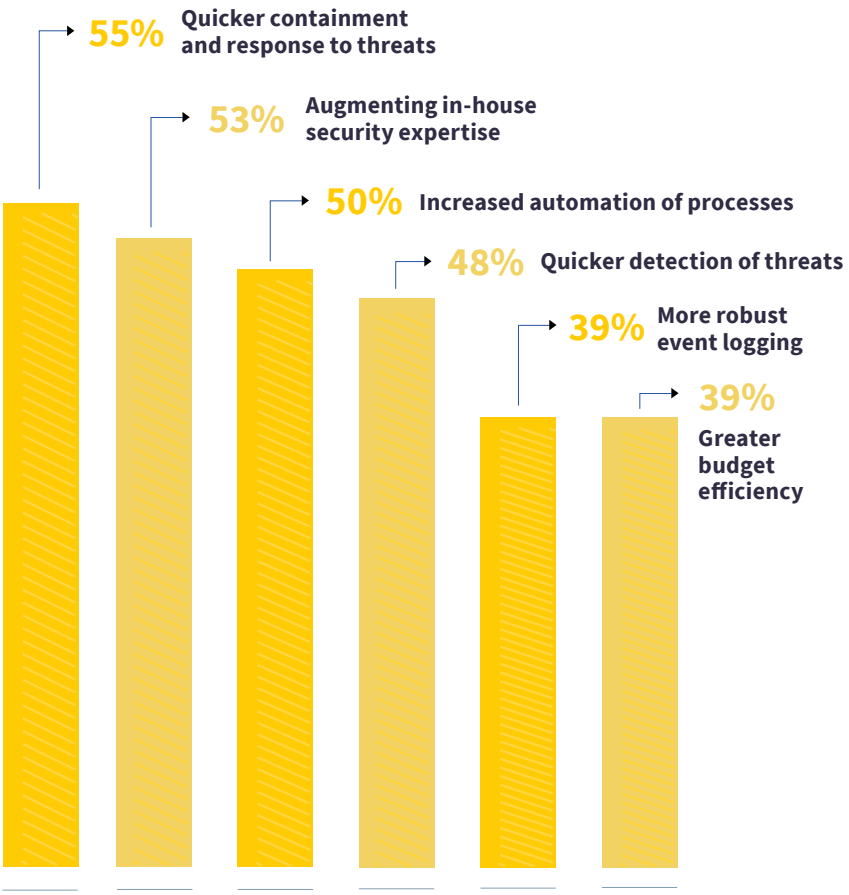
Nearly every organization surveyed (99%) has plans to automate some aspect of incident response in the next year ...		... but automation remains hindered by various obstacles, in particular:	
Automating threat detection	68%	Lack of in-house expertise	47%
Automating threat analysis and investigation	74%	Lack of supporting tech or platforms	
Automating threat containment and remediation	72%	Excessive time commitments	

To address these shortcomings, security leaders are increasingly recognizing the benefits of third-party partners that provide managed detection and response. With security teams inundated with alerts, adding extra people is not always the most efficient, or practical, option. Instead, a partner can have an impact across the incident response process, particularly in the areas that security leaders want to improve most. Leaders see third-party providers as most beneficial for quicker containment and response to threats (55%), augmenting in-house security expertise (53%), and increased automation of processes (50%).

Leaders are looking for new partners to help leverage these benefits. Four in five (82%) say they will likely work with a new partner to assist with their incident response process, indicating that third parties will continue to play a growing role going forward.

BENEFITS OF MDR PROVIDERS

*Stats are referencing responses from security leaders



As security leaders look for a new partner, two factors are particularly crucial. For 86%, it is important that a partner can handle multiple aspects of threat management, specifically 24/7 response, containment, and remediation of threats by trained experts. For 87%, the most important factor is that the partner can provide automated tools to reduce the mean time to respond to threats.

> “Organizations are more aware of threat activity, but that’s not making their security problems go away. Security leaders are still looking for partners to augment their 24x7 security operations, with about half of them recognizing they need additional capability to gather and respond to investigative findings.”

Grant Oviatt
Director of Incident Response Engagements
RED CANARY

Conclusion

Security teams around the globe have responded brilliantly to the unprecedented challenges they've faced over the past year, but the immense pressure that teams are under doesn't show signs of letting up anytime soon. With one dangerous attack following the other, the time to act is now. There's ample opportunity to improve on processes that may have been put in place in a hurry, or those that may have simply become outdated.

It's as good a time as any for security teams to reevaluate their detection and response capabilities, adopt new best practices, shore up incident response plans, and bring in trusted partners to help fill in any gaps in resources or expertise. Based on the findings of this research, here are several actionionable steps organizations can take today:

Build a secure foundation

No organization is immune to cyber attack. Ensure the foundational security controls are in place to help you catch threat activity before it becomes a significant problem for your organization. Strong identity protection like multi-factor authentication remains vital in slowing adversaries, as it better secures the weakest link in any security organization's posture: humans.

Test the process, close the gaps

Given the importance of incident response, testing the process should be of the utmost importance, especially given the significant number of respondents reportedly lacking adequate tools, having insufficient expertise on staff, and spending too much time investigating low-level alerts. Security leaders are turning to a variety of methods for assessment, but many are overlooking vital practices. Conduct incident response exercises on a regular basis, update your incident response process based on frameworks like NIST, and measure any changes in performance based on the response to actual incidents.

Adopt security best practices

Organizations not following best practices in their security operations aren't setting themselves up for a high likelihood of success. While introducing best practices and formal strategies won't automatically make an organization more secure, it will provide a clear structure and enable easier measurement of security processes' effectiveness.

Build a bridge to legal counsel

Legal implications of being breached remain uncertain to many organizations, with almost half the survey respondents reporting a lack of clarity on when to engage counsel about a potential breach. By fostering collaboration between infosec and legal, organizations can eliminate this uncertainty and create an easy pathway for staff to follow to get quick answers when an attack is underway and time is of the essence.

Partner with third-party providers

Security leaders are increasingly recognizing the benefits of third-party partners that provide managed detection and response. With security teams inundated with alerts, adding extra people is not always the most efficient, or practical, option. Bringing on a third-party provider as a partner can have an impact across the incident response process, particularly in the areas that security leaders care about the most: improving time to containment and response to threats, augmenting in-house security expertise, and increasing automation.

> “Compliance and models don't inherently make you safer. But they do provide you with structure, make it easier to measure and communicate what your program is doing, and they also make it harder to 'forget' to do things that you decide are important, like performing compliance audits of partners or regularly drilling your incident response team/process.”

Keith McCammon
Chief Security Officer
& Co-founder
RED CANARY

About the data

The Kroll, Red Canary, and VMware Carbon Black State of Incident Response Survey was conducted by Wakefield Research among 500 security leader respondents from companies with personnel/staff of 700 or more and revenue of more than $500 million, between November 16 and December 2, 2020.

The security leader audience is comprised of two sub-groups:

- **IT/Information Security** (n=400): respondents with the titles of CIO, CISO, CSO, CTO, and Director of Security, Information Security or IT
- **Corporate Counsel** (n=100): respondents with the titles of Chief Legal Officer, General Counsel, Chief Compliance Officer, Chief Privacy Officer, EVP/VP of Legal Affairs or Legal/Compliance/Privacy Manager

The overall margin of error for this study is +/-4.4 percentage points at the 95% confidence level. Base sizes under 100 are considered small and associated findings are directional.

KROLL

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit **www.kroll.com**.

red canary

Red Canary is the leading security ally enabling every organization to make its greatest impact without fear of cyber-attack. The company provides outcome-focused solutions for security operations teams, who rely on Red Canary to analyze and respond to endpoint telemetry, manage alerts across the network, and provide cloud environment runtime threat detection. With Red Canary, security teams can make a measurable improvement to security operations within minutes. To learn more, visit **redcanary.com**.

vmware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit **www.vmware.com/company**.