White Paper, sponsored by Commvault | September 2023

THE CYBER-RESILIENT ORGANIZATION:

Maximum Preparedness with Bulletproof Recovery

Phil Goodwin
Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

IDC Opinion

Cyberattack may be the biggest existential threat faced by IT organizations throughout the world today. Cyberthreats evolve rapidly, and tomorrow's threat landscape may look nothing like what we imagine today. While detection, prevention, and recovery technology is advancing rapidly, the methods used by cyberattackers are becoming ever more sophisticated. Artificial intelligence (AI) may improve our detection and response capabilities, but it may also assist cybercriminals in their attacks. Because of the high stakes and risks associated with cyberattacks, organizations must focus on becoming cyber-resilient. This means not only planning to recover or creating a defensive perimeter but also developing a fully integrated posture of proactive preparedness and robust "bulletproof" recovery capabilities.

Cyber-resilience involves two key efforts: intrusion prevention and intrusion recovery.

Unfortunately, many organizations suffer significant losses and business consequences from cyberattacks. We believe that some of the reasons for these issues include:

- Data sprawl, whereby data is spread across on-premises, cloud, and edge repositories, leading to higher risk of intrusion and more difficulty applying cyberdefense
- Lack of standardized cyber-recovery tools and processes across the various repositories, complicating responses
- Organizations' taking a tactical approach to intrusion detection and recovery rather than treating it as a long-term strategic initiative
- Lack of coordination between ITOps and SecOps teams, leading to siloed preparedness efforts, often the result of diverse leadership structures

Cyber-resilience involves two key efforts: intrusion prevention and intrusion recovery. No amount of prevention can guarantee that an intrusion will not occur. Organizations routinely report hundreds or even thousands of attack attempts per day, especially in certain sectors such as financial services. The odds are simply in the favor of attackers: They can fail 99% of the time and still be successful, whereas anything less than 100% success for defenders can be catastrophic. Because intrusion is always a possibility, organizations need 100% "bulletproof" recovery capabilities to recover quickly, avoid data loss, and eliminate the need to pay a ransom.

Methodology

Commvault sought to learn how organizations are approaching cyber-resilience, what gaps in cyber-responses are common, and best practices as learned and described by senior IT professionals. To facilitate this research, Commvault commissioned IDC to conduct an independent effort to find answers to these important issues.

The research methodology used by IDC was the most comprehensive methodology possible, involving all three primary research methodologies: a focus group of eight IT leaders of major U.S. companies (several multinationals) with CIO, CTO, and CISO titles; individual in-depth interviews of other CIOs; and a worldwide survey of senior IT and security professionals with an n = 513.

Findings

Surveys offer statistically meaningful data across large audiences. In this case, our 500+ respondents represented a worldwide audience from North America, Europe, Africa, South Asia, and Australia/New Zealand. The respondents were all from medium- to large-scale organizations with 2,500 or more employees, spread across 23 industries.

The advantage of focus groups as research tools is the ability to drill deep into topics and generate extensive commentary. In addition, participants may have different perspectives, allowing a broader discussion of the issue. In this case, all focus group respondents were C-level executives directly involved in their organization's cyber-resilience strategies and implementation. Key findings from these combined research efforts are described below.

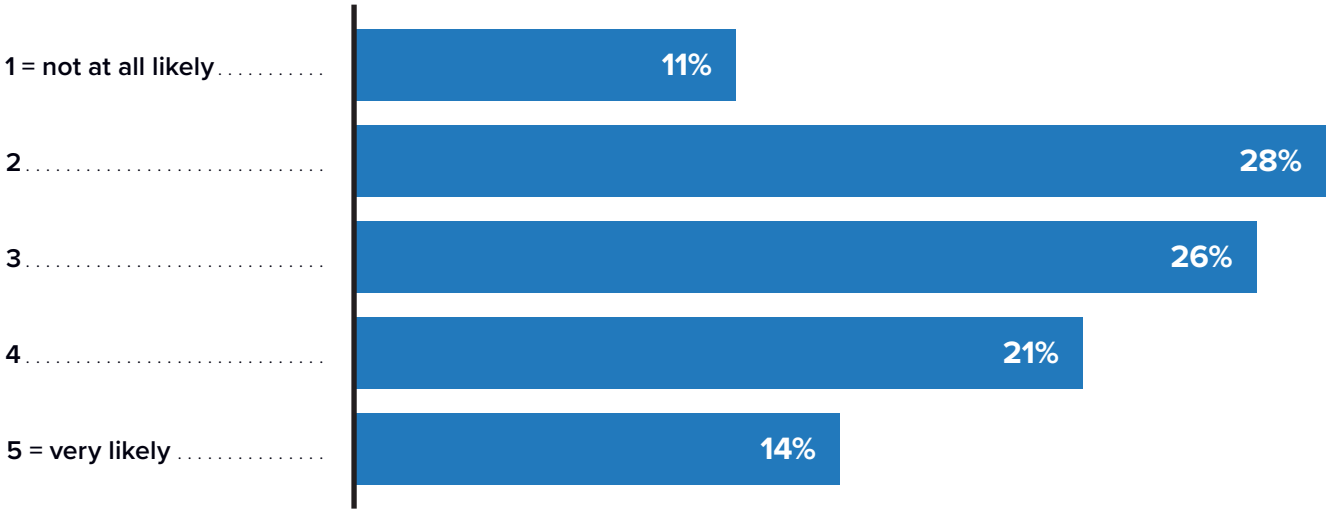
Finding: Data and workloads remain at constant risk

IT and business leaders alike understand the constant risk of cyberattacks, and most understand the risks and consequences. In our survey, 61% of respondents believed that data loss within the next 12 months due to increasingly sophisticated access is "likely" to "very likely" (lines 3–5 in **Figure 1**); only 39% found such a scenario to be "not very likely" or "not at all likely" (lines 1–2 in **Figure 1**).

FIGURE 1

Likelihood of Data Loss in the Next 12 Months due to Increasingly Sophisticated Cyberattacks

(Percentage of respondents)



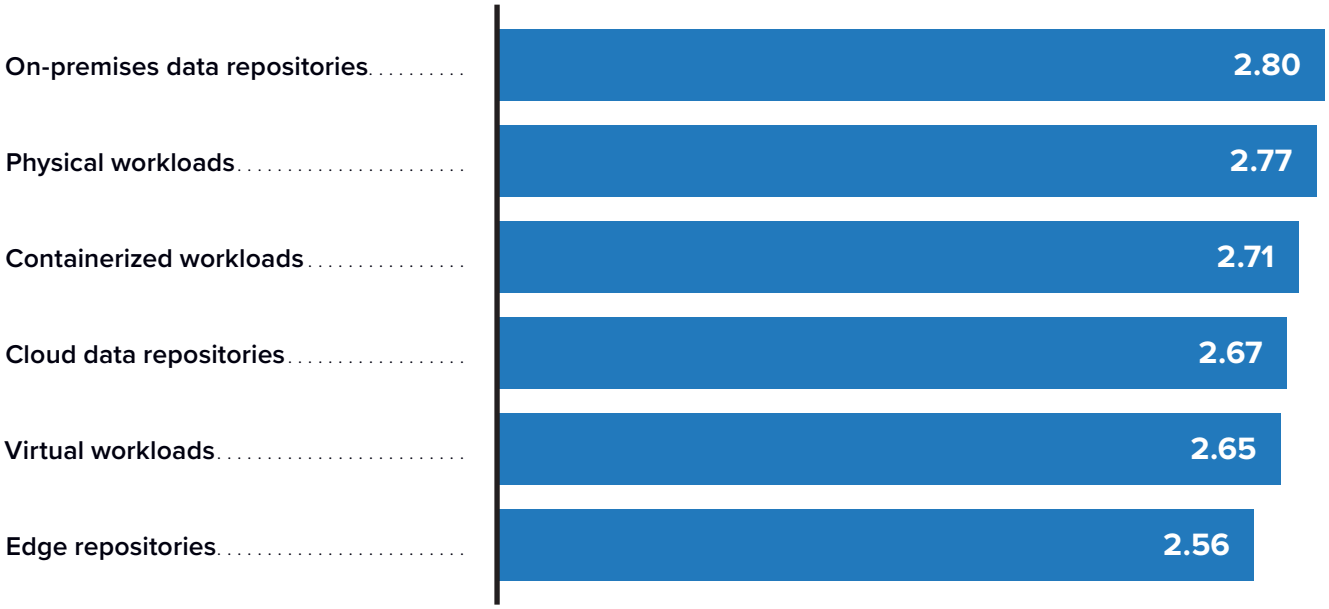
n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023
Scale: 1 = not at all likely, 5 = very likely

The fact that organizational leaders recognize this risk is less surprising than the areas in which they perceive the highest risk. Given the historical anxiety over the security of cloud workloads, we were surprised to learn that on-premises and physical workloads are viewed as the most vulnerable. **Figure 2** (next page) shows these results. (Note: Scale is 1 = not vulnerable at all and 5 = very vulnerable).

FIGURE 2

Workload Vulnerability

(Mean)



n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023
Scale: 1 = not vulnerable at all, 5 = very vulnerable

We believe this finding is because the majority of cyber-recovery and preparedness solutions are aimed at virtual infrastructure; relatively few are aimed at physical on-premises workloads. These types of workloads are often hosted on mission-critical systems with Unix or other operating systems. Thus, for those organizations with a mix of virtual, physical, and legacy workloads, it is important to consider solutions that are capable of addressing all of the organizational cyber requirements.

Finding: "Bulletproof" recovery is paramount

Cyber-resilience activities can be loosely grouped into two areas: prevention and mitigation. Our focus group panelists agreed that no organization can ever be 100% sure of preventing an attack. Thus, the ability to recover cannot be compromised. One of the panelists summed it up:

> *No matter how much effort I expend on detecting and preventing, I still have to know I can recover, and I need to be able to tell my execs and my board that yes, we have that capability and it's been tested. It needs to be bulletproof here, because you'll never be bulletproof on detecting and protecting."*
>
> — Senior VP of information technology/CIO/CISO, real estate

IDC considers this level of recoverability as foundational to cyber-resilience, making backup and recovery the centerpiece of any cyber-resilience strategy. Nevertheless, a backup product alone is not enough. To be effective for cyber-resilience, data security products must integrate with products in the cyber-recovery ecosystem, including detection/diversion capabilities (e.g., malware detection, honey pots), reporting capabilities (i.e., security information and event management [SIEM] and security orchestration, automation, and response [SOAR] tools), audit tools, and so on.

Finding: Testing and validation are essential

Disaster recovery testing and cyber-recovery testing are too often overlooked and under-addressed by organizations, primarily because they are so time-intensive and intrusive to the organization. With cyberattack being a "when" rather than an "if," validating a recovery system could not be more important. According to one of our panelists:

> *When it comes to backups and things like offline backups and online backups, I would say what we don't do well is testing the integrity of the backup."*
>
> — CTO, construction

Again, recovery validation is the key. Organizations need to know, to a high degree of confidence, that their recovery strategy will be successful. Different testing methods are available, with these three being the most common:

- **"Preflight" check:** A preflight check is a mechanism that can check the source and target recovery environments for consistency, appropriate configuration, and compatibility. It also checks for up-to-date software and drivers and for other issues that could cause a failover failure.
- **Simulated test:** Simulation software executes a failover test plan without physically moving any data or workloads. Simulated tests are generally nondisruptive to the organization because production systems run without interruption. Simulations can find failure points not seen in a preflight check.

- **Physical test:** Physical tests involve the actual failover of data workloads from production infrastructure to recovery infrastructure. They are disruptive to the organization, as systems may be temporarily unavailable during the failover.

Because physical testing is time-consuming for IT and disruptive to the business, most organizations do it rarely or not at all. However, testing is essential to giving organizations the best chance of recovery success. Those with the most mature efforts combine preflight checks on a frequent basis with at least quarterly simulated tests and a full physical test at least once per year. As one of our panelists stated:

> *"A lot more attention goes to protecting and detecting data breaches. It feels more active. It feels more of an everyday type thing. The other [recovering data] should have everyday attention as well, but you sort of assume it's happening. Yes, you do testing, and hopefully when that moment comes, all of your testing has proven that yes, it is recoverable and it hasn't been compromised."*
>
> — CIO, healthcare

To illustrate the importance of testing and validation, our survey found that 59% of respondents expect cyber-recovery efforts to take days or weeks to complete. Only 41% believed they could recover in less than 24 hours. Proper testing and validation can help avoid the consequences of lengthy recoveries, such as loss of revenue, loss of customers, cost of downtime, and so on.

Finding: Cyberattack preparation and response require a coordinated effort between ITOps and SecOps

The SecOps team has primary responsibility for intrusion detection and prevention but little visibility into recovery requirements and systems. Conversely, the ITOps team is responsible for restoring data, systems, and applications in the event of a successful cyberattack. Unfortunately, our survey found that these groups are too disconnected. Only 30% of SecOps teams fully understand ITOps roles and responsibilities, and only 29% of ITOps teams fully understand SecOps roles and responsibilities.

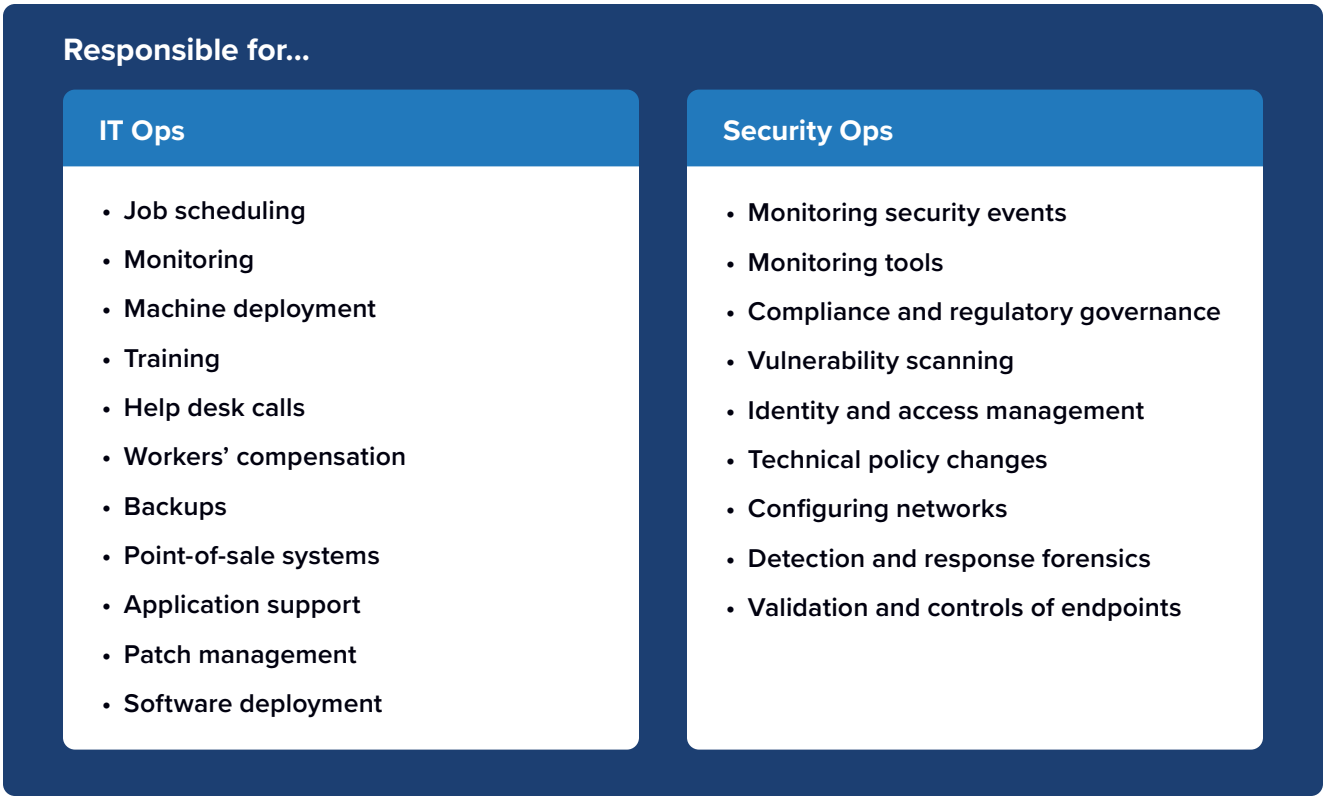
Our focus group panelists characterized this division as SecOps being responsible for the strategy and ITOps responsible for the tactics. According to one panelist:

> *Security seems to be more on the strategic side — what we have to do, writing the policy — and the IT side for us is the implementer. They put [the solution] in place. They put the architecture in place. I have them sitting right next door. Their offices are right next to each other. It's a concept in communication."*
>
> — CIO/CISO, real estate

When asked to assign responsibilities to the respective teams, our panel yielded the results illustrated in **Figure 3** (next page).

FIGURE 3

ITOps and SecOps Responsibilities



Source: IDC 2023

We learned from our focus group that there is little industry consistency regarding the actual organization of SecOps and ITOps teams. Some have SecOps reporting to the CISO and ITOps to the CIO, others involve the CTO with either or both teams, and some have a single leader for all, usually the CIO. Smaller organizations are more likely to have a single leader for both teams, whereas larger organizations are more likely to have them split. Regardless of organizational structure, having well-coordinated teams where each understands the other's role improves cyber-resilience outcomes. According to one of our panelists:

"We have to talk constantly. We have meetings on a daily basis around our backups and anything going on with that. We also talk constantly about how the environment is performing and how we can improve that environment. We work directly — both sides work directly with the business if there needs to be a recovery of any data or a restoration of that data from a legal perspective."

— CISO/VP of security, financial services

To effectively leverage this communication, however, organizations need integrated toolsets spanning the two teams. For example, having backup system detection and monitoring software that feeds data and alerts into SEIM tools can ensure that any anomalous behavior is immediately reported and acted upon. Any method that helps rapidly detect attacks minimizes the impact and shortens the recovery time. According to our panelists, automation can play a key role in better collaboration:

> *"The only thing I can think of that would [improve] collaboration is any type of automation. … Then you really take the human factor out of it. I try to think of anything where there's an operational duty. If I develop the process good enough and I can take the human factor out of it, then [maybe] I don't need a person. If I can automate that process, that lets them go on and do other things besides operational duties."*
>
> — CISO, consumer goods

Finding: Cyber-resilience starts in the C-suite

Our panelists agreed that cyber-resilience requires a company-wide effort, and that effort starts at the top. Without executive sponsorship and visibility, it is too tempting for line-of-business (LOB) teams to assume that cyber-preparedness is limited to the IT team. This problem was expressed by one of our panelists this way:

> *I don't think the line of business cares until [applications] are not there. It's like a light switch: walk in, should turn on every day. The day it doesn't turn on — now we've got a problem. They are thinking about other things, about running the business, not about this, even though this is integral to the business."*
>
> — CIO, healthcare

Another panelist described their stance toward involving executives in preparedness:

> *"We take a very strong strategic approach [for data security] all the way to the top. There is a very strong focus from the board — what we are doing, how we are doing it. There are a lot of discussions around it."*
>
> — CIO/CISO, real estate

With board-level attention to cyber-resilience and preparedness, line-of-business leaders will be fully aware of the issue and their responsibilities in supporting resiliency efforts. In fact, all eight panelists identified phishing as the most

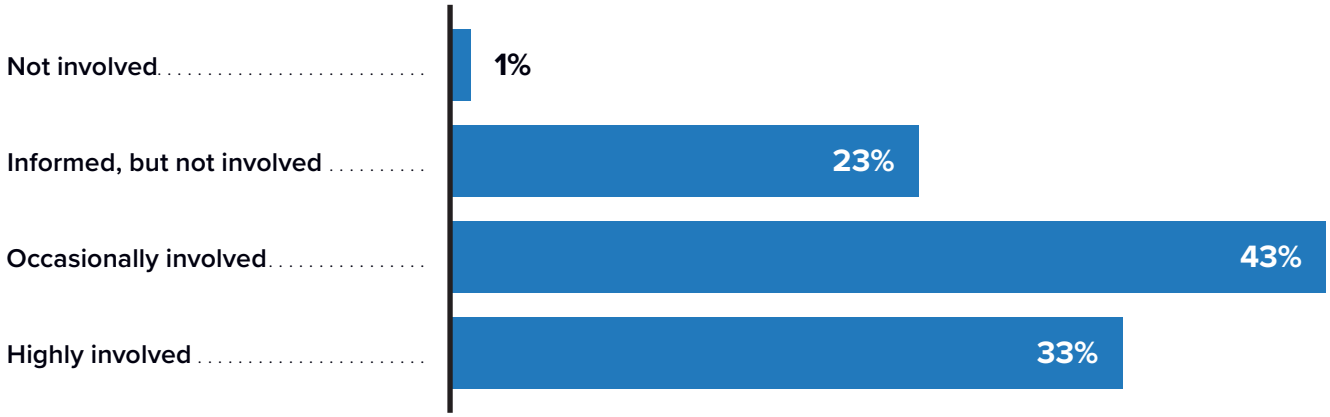
concerning threat to address, given that most ransomware attacks begin with a successful phishing attack to compromise user credentials. Training, awareness, and the proper malware detection tools are the best defense against such attacks.

Unfortunately, our survey found that the top leaders in the organization are not always as involved as perhaps would be optimal. First, we found that the CEO or managing director (MD) is heavily involved in only about one third of situations. These results can be seen in **Figure 4**.

FIGURE 4

CEO and Managing Director Involvement in Cyber-Preparedness

(Percentage of respondents)



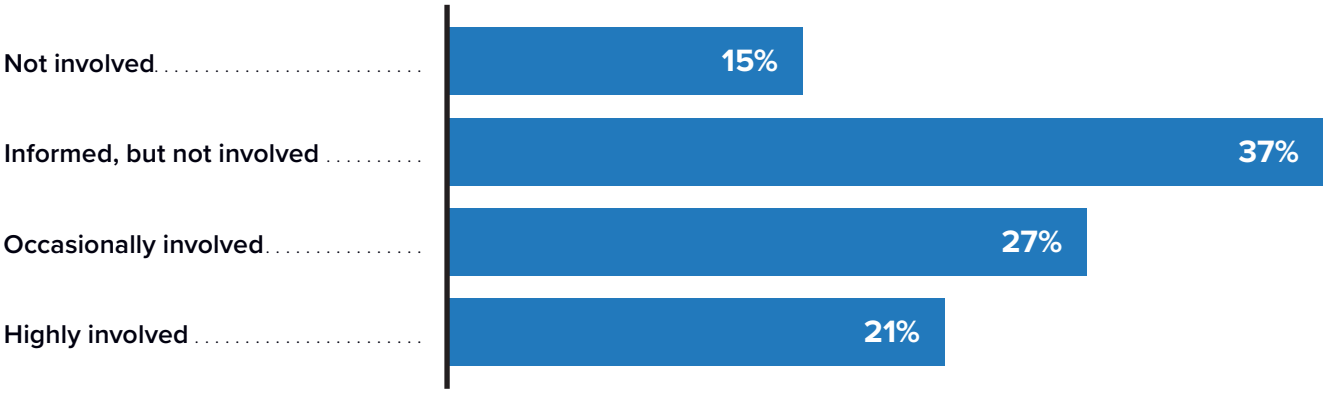
n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023

We can see from this data that the CEO/MD has very little involvement in about one quarter of cases. Without this senior level of involvement, cyber-preparedness efforts risk not being viewed as a priority to rank-and-file team members, and this lack of priority may extend to insufficient funding. Furthermore, our survey found that senior line-of-business leaders are even less involved (see **Figure 5**, next page).

FIGURE 5

Line-of-Business Leader Involvement in Cyber-Preparedness

(Percentage of respondents)



n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023

As this chart shows, LOB leaders are highly involved in less than a quarter of cases and essentially not involved in 52% of cases. To amplify what we learned from our panelists, LOB leaders cannot suddenly become interested after the organization has been attacked; they must be involved in the preparation efforts so that all employees take training and awareness seriously. Without thorough training and awareness, organizations increase risk of attack and are more likely to experience longer recoveries.

Finding: Rapid detection lessens impact and speeds recovery

Three of our panelists had suffered a cyber-intrusion. Each indicated that their team had detected the attack in 30 minutes or less, but even those short attack times resulted in damage that required a recovery response. Moreover, even with rapid detection of a cyberattack, recovery time can be proportionally much longer, as this panelist indicates:

"I think for us it was probably about 10 minutes to detect [the attack] and then immediately we were able to contain it, but the recovery took six hours just because of the type of data that was involved."

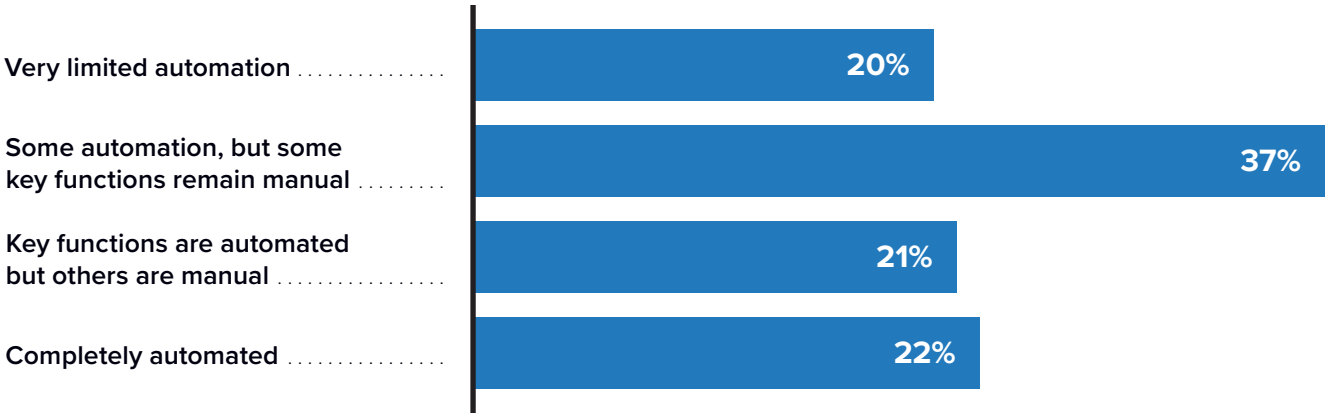
— CISO, transportation

Speed of detection is clearly key to mitigating intrusion impact, and detection, in particular, requires automation to be effective. However, it appears that most organizations are still on the journey to fully automated detection and reporting, as the results in **Figure 6** demonstrate.

FIGURE 6

Degree of Automation in Cyber-Detection and Reporting

(Percentage of respondents)



n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023

From this data, we can see that only 22% of respondents reported being fully automated, while 57% have limited automation for key functions. As cyberattackers deploy more clever attacks, relying on manual detection and reporting processes is very likely to result in missed anomalies and successful attacks.

Finding: Comprehensive cyber-preparedness impacts cyber insurance policies and premiums

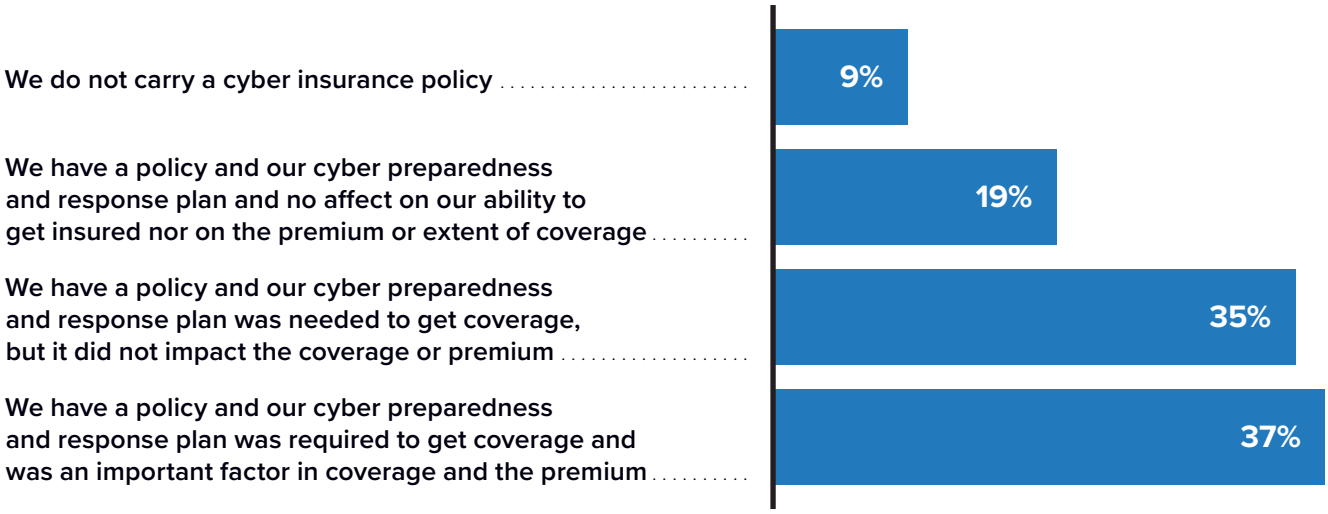
Cyber insurance is gaining in popularity as the cost of cyberattacks increases. Cyber insurance plans can vary widely, but they are generally intended to cover costs of downtime, lost business, or other impacts. Because the cyber guarantees offered by some vendors are usually limited in scope to the cost of data recovery and do not address these other costs, getting cyber insurance may be prudent for many organizations.

We asked the respondents into our survey to tell us if having a comprehensive cyber-preparedness plan had an impact on their ability to get a cyber insurance policy or if it had an impact on premiums. The results were overwhelming. As **Figure 7** shows, only 9% of respondents did not have cyber insurance. Of the remainder, 19% said a cyber plan had no impact, but 35% said it was important to getting coverage, and 37% said it was important both to getting coverage and to their premium. Clearly, many insurers have strict requirements for getting coverage, and some will charge more for less-prepared policyholders.

FIGURE 7

Importance of Cyber-Preparedness to Cyber Insurance Coverage and Premiums

(Percentage of respondents)



n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023

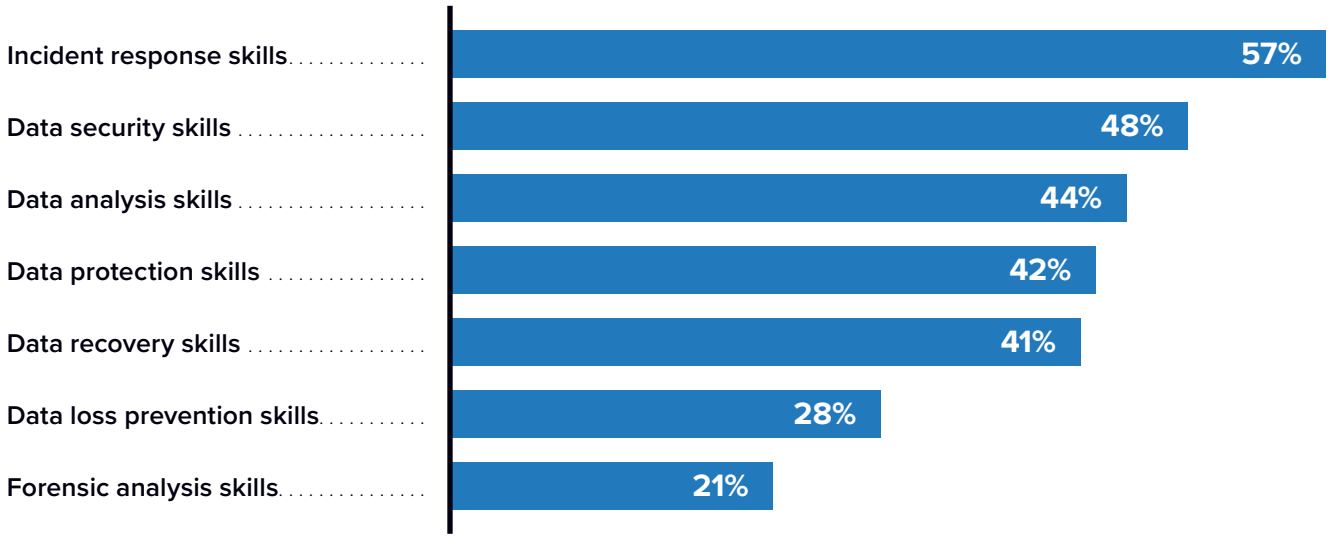
Finding: Incident response skills are the most lacking

IT organizations commonly have skills gaps, especially for growing problems such as cyberattacks. We asked survey respondents to tell us which skills they would be looking for most in the next 12 months. Incident response (IR) skills was the top choice, with 57% of respondents choosing it. This was the only skill that garnered more than half of the respondents. **Figure 8** provides the details.

FIGURE 8

Top Skills Needed in the Next 12 Months

(Percentage of respondents)



n = 513, Base = all respondents; Source: IDC Custom Survey sponsored by Commvault, August 2023

While attaining these skills is important, some cyber-protection vendors offer consulting services and incident response teams that can be engaged to assist in the event of a cyberattack. The advantage of these teams is a breadth of experience across numerous cases and familiarity with various attack methods and the best, fastest way to recover from them. In fact, we believe organizations will increasingly turn to engaging IR teams, as "DIY" IR efforts prove to be lacking in speed and effectiveness.

Future Outlook

Ransomware and other malware attacks have become a fact of life. It is simply too profitable for criminals to abandon as long as it continues to pay. Our research also finds that data exfiltration attacks occur about 50% more often than encryption attacks. We believe this is because there is no recovery from an exfiltration event. Organizations simply determine whether or not to pay the ransom. If the attacker can get valuable data, then the chances of a payment increase.

More recently, criminals have started to pursue "dual threat" attacks. In these attacks, the criminals attempt to both exfiltrate the data and encrypt it. If successful, it increases pressure on the company to pay and increases the possible ransom value. If IT teams focus only on recovery, they become vulnerable to exfiltration schemes.

To enhance an organization's resilience posture, IDC recommends the following best practices:

1. **Protect the backup first.** Cybercriminals have learned that deleting or compromising backups increases the chances of ransom payment. Our research shows that backups are attacked in about 50% of cases, with nearly half of those being successful. It is also important to secure the backup environment, because attackers may change backup policies, delete backup jobs, change retention schedules, or change immutability policies that do not appear as overt attacks.
2. **Encrypt data.** Data encryption at rest and in flight is the best defense against data exfiltration. It is also the best defense against the "prying eyes" of internal threat actors. This applies especially to backup data.
3. **Make data copies immutable.** Data (especially backup data) that cannot be deleted or altered is one of the best assurances for data survival. The strongest form of immutability is one where even superusers cannot make changes.
4. **Create air-gapped data copies.** An "air gap" is the physical separation of backup from networks that attackers can access. Data on tape, removed from a device, is a strong air gap. In system-based air gaps, the data path should be separate from the control path to make it harder for attackers to gain access to both. Simply tiering data to the cloud is not an air gap and offers a false sense of security.
5. **Use a 3-2-1-1 backup strategy.** This means three copies of the backup on two separate types of media with one onsite/offline copy and another offsite/offline copy. These latter copies are often air-gapped.

6. **Implement zero-trust architecture.** Zero-trust architectures can limit the scope of cyberattacks when implemented correctly. In the case of backup environments, this includes such things as multifactor two-factor authentication (MFA) to sign in and two-person authentication to change backup, retention, and immutability policies. Our research shows that only about 40% of organizations claim to have implemented zero-trust. However, zero-trust is not all-or-nothing; organizations can implement one aspect at a time and significantly improve the resilience posture. Role-based access control (RBAC) also limits an individual's ability to access sensitive information without specific authorization.
7. **Treat incident response strategically.** Organizations should recognize that incident response, including recovery preparation, is as strategic as data security. The two must go hand in hand rather than be treated as separate activities.

Challenges/Opportunities

Cyber-resilience requires a coordinated and sustained effort of people, process, and technology. Organizations may be tempted to lean too heavily on technology, but there is no silver bullet to cyber-recovery. Moreover, no single product can address every contingency. A major challenge for data security vendors, including Commvault, is the difficulty of keeping up with and defending against evolving attacks. It is also important for such vendors to participate in the broader cyber-protection ecosystem, such as malware detection and scanning, SEIM/SOAR tools, forensic analysis, and more. This can pull a vendor in many directions, and getting it right is imperative.

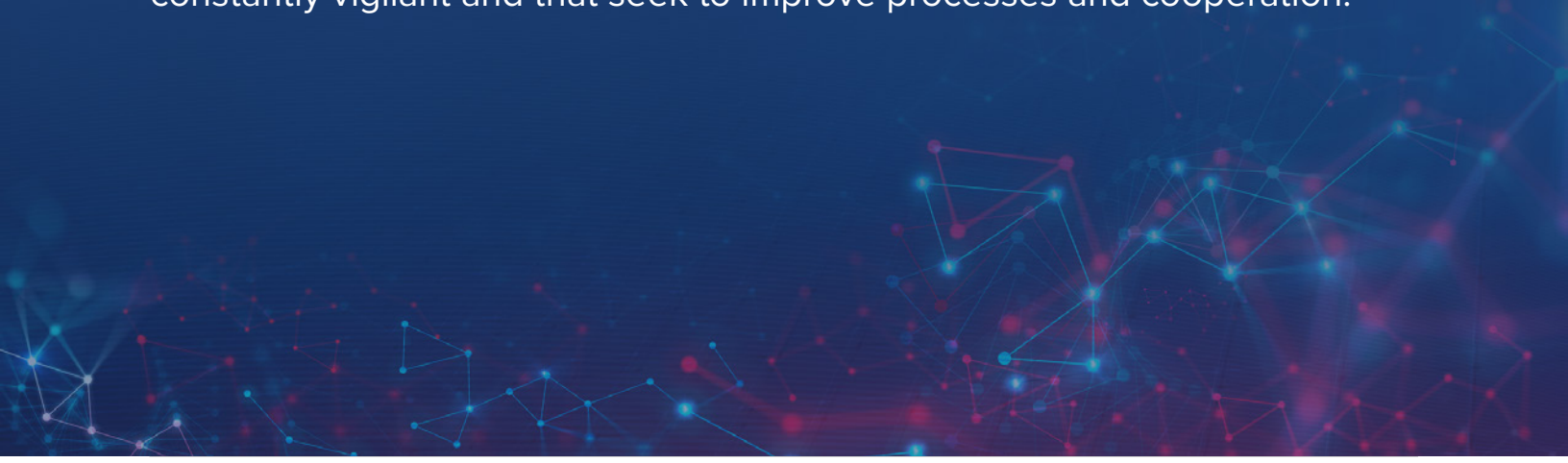
Going forward, we expect AI to play a significant role in cyber-protection and recovery. Indeed, we expect cybercriminals (especially those who are state-sponsored) to leverage AI to gain attack leverage. Data security vendors are well positioned to implement AI, because it can be used to spot unusual data access or backup behavior, develop dynamic runbooks that update with configuration changes, and provide precise, on-the-fly recovery orchestration. This is an arms race, and Commvault must strive to be at the forefront of the industry.

Conclusion

Cyber-preparedness is a top priority of organizations worldwide, as cyberattack knows no borders and spares no organization. Fully prepared organizations do everything they can to keep attackers out, but they recognize that attacks are nearly inevitable. Thus, having absolute "bulletproof" recovery capabilities is both essential and foundational to cyber-preparedness. Without this recovery capability, organizations risk serious business consequences when attacked.

Cyber-preparedness involves many layers of protection. This includes endpoint protection, network security, automated detection and reporting, data encryption, data immutability, zero-trust principles, and orchestrated recovery. Our findings from this research show that technology is critical but is not enough; preparedness starts with executive teams committed to preparedness and ITOps and SecOps teams that are constantly vigilant and that seek to improve processes and cooperation. These highly committed organizations can expect better outcomes following a cyberattack with minimized business impact, no loss of data, and the fastest possible recovery.

Technology is critical but is not enough; preparedness starts with executive teams committed to preparedness and ITOps and SecOps teams that are constantly vigilant and that seek to improve processes and cooperation.



About the IDC Analyst

Phillip Goodwin

Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Phil Goodwin is a research vice president within IDC's Infrastructure Systems, Platforms and Technologies Group, with responsibility for IDC's infrastructure software research area. He provides detailed insight and analysis on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption. His focus is on multi-cloud data management, data logistics, on-premises and cloud-based data protection as-a-service, cyber protection and recovery, recovery orchestration, and more. Phil takes a holistic view of these markets, and covers risk analysis, service level requirements and cost/benefit calculations in his research. He also contributes regularly to IDC's CIO advisory practice.

More about Phillip Goodwin

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

@idc @idc idc.com

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.