b!nalyze

Preparing Your Incident Response Team for Cyber Resilience

Introduction: How much are you thinking about cyber resilience?

Are you thinking about how resilient your organization is against cyber threats and attacks in 2024?

You should be!

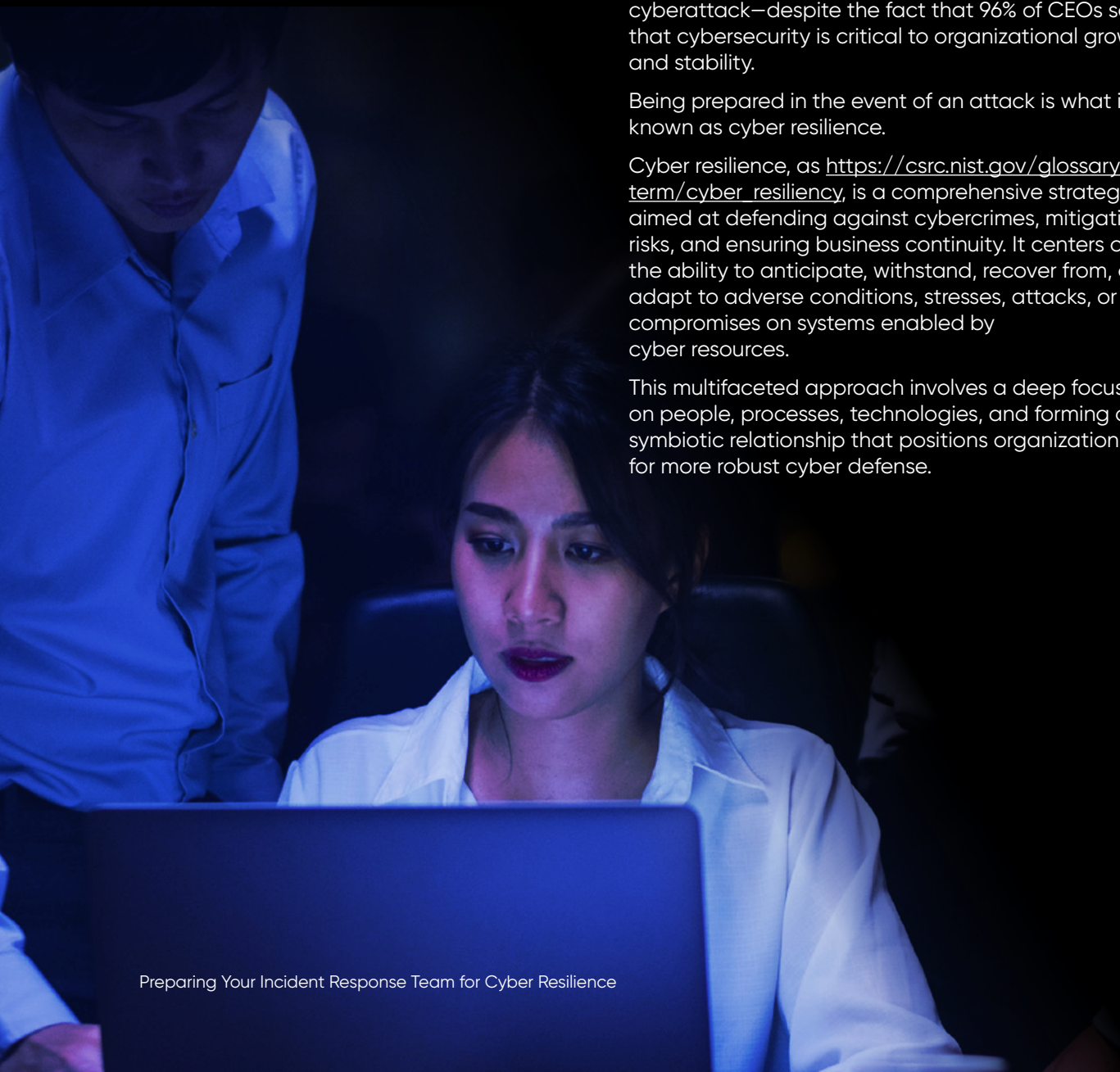
Put simply, executive management is also wondering about your security posture – and how capable you are of recovering quickly in the event of a security incident.

Research from Accenture finds three-quarters (74%) of CEOs are concerned about their organizations' ability to avert or minimize damage to the business from a cyberattack—despite the fact that 96% of CEOs said that cybersecurity is critical to organizational growth and stability.

Being prepared in the event of an attack is what is known as cyber resilience.

Cyber resilience, as https://csrc.nist.gov/glossary/term/cyber_resiliency, is a comprehensive strategy aimed at defending against cybercrimes, mitigating risks, and ensuring business continuity. It centers on the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems enabled by cyber resources.

This multifaceted approach involves a deep focus on people, processes, technologies, and forming a symbiotic relationship that positions organizations for more robust cyber defense.



Why do organizations need to be cyber resilient?

Security leaders are tasked with balancing the protection of their organization through a cybersecurity and risk mitigation strategy – as well as keeping on top of business operations and digital transformation efforts.

The accelerated adoption of new technologies has led to a complex IT ecosystem and a constantly expanding attack surface. Any CISO or security leader worth their salt knows that trying to keep up with criminal adversaries is like playing a never-ending game of cat and mouse. Any time security innovates a new way to defend themselves; criminals adapt new techniques for exploitation.

This challenging environment is coupled with industry-wide staff and skills shortages of both experienced cybersecurity professionals and new trainees entering the talent pool recent research from the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) reveals 71% of security pros say their organization has been impacted by the global cybersecurity skills shortage - up from 57% in 2021. Add to that the challenges of security analyst burnout, with 59% of cybersecurity analysts saying that they plan to quit their jobs despite high industry wages.

All of these factors combined mean that 100% breach protection is no longer a realistic expectation. That's why recognizing the inevitability of compromise or data breaches is fundamental to attaining cyber resilience.

Additionally, cyber insurers and regulators are watching. There is increasing pressure on organizations to demonstrate proactive activities, including vulnerability management, incident response planning, plan testing, pen testing, vulnerability assessments, compromise assessment, and threat hunting.

Becoming truly cyber resilient requires a move beyond security prevention towards improving incident response capabilities and tooling for preparedness, response, and quick recovery. Enter your incident response team (IR) and other security defenders, who play an integral role in your cyber resilience strategy.

Incident response readiness - A key component of cyber resilience

Incident response readiness plays a pivotal role in achieving cyber resilience, requiring a combination of the right technology, the right team, and the right processes. The ability to respond swiftly or prevent further incidents hinges on having these components in place.

A proactive and comprehensive approach to incident response not only minimizes the impacts of cyber incidents but also strengthens an organization's ability to adapt and withstand the ever-evolving cyber threat landscape. In a rapidly changing digital environment, incident response readiness is not just a necessity; it is a strategic imperative for any organization committed to reducing cyber risk and costs alongside safeguarding its data, reputation, and overall business continuity.

All about Digital Forensics and Incident Response (DFIR)

Incident response readiness plays a pivotal role in achieving cyber resilience, requiring a combination of the right technology, the right team, and the right processes. The ability to respond swiftly or prevent further incidents hinges on having these components in place.

A proactive and comprehensive approach to incident response not only minimizes the impacts of cyber incidents but also strengthens an organization's ability to adapt and withstand the ever-evolving cyber threat landscape. In a rapidly changing digital environment, incident response readiness is not just a necessity; it is a strategic imperative for any organization committed to reducing cyber risk and costs alongside safeguarding its data, reputation, and overall business continuity.

DFIR involves the collection, analysis, and preservation of electronic evidence to investigate and respond to cyber incidents. It has a crucial role in identifying, containing, and mitigating the impact of security incidents, such as data breaches, malware infections, and other cyber threats.

There are two main components of DFIR:

Digital Forensics:

- **Collection of Evidence:** Digital forensics involves gathering and preserving electronic evidence from various sources, such as computers, servers, network logs, and digital devices.
- **Analysis of Evidence:** Forensic analysts examine the collected data to reconstruct events, identify the root cause of incidents, and gather information. For example, for legal proceedings, if necessary.
- **Chain of Custody:** Maintaining a secure chain of custody is critical to ensure that the integrity of the evidence is preserved, making it admissible in legal proceedings. For example, RFC3161 digital timestamp certification.

Incident Response:

- **Detection and Identification:** Incident response focuses on quickly detecting and identifying security incidents. This includes activities such as monitoring network traffic, analyzing logs, and using intrusion and threat detection systems.
- **Containment and Eradication:** Once an incident is identified, the goal is to contain it to prevent further damage and eradicate the threat from the affected systems.
- **Recovery and Post-Incident Analysis**: After containment, the focus shifts to recovering affected systems and conducting a thorough analysis of the incident to understand its scope, impact, and tactics used by the attackers.

  Collecting and using the right level of digital evidence is crucial to help incident response investigators fill gaps in information about cyberattacks, such as who the attackers were, how the incident happened, and how to remediate any security holes.

  Strong DFIR capabilities can also help identify the data lost or the exact damage caused, which is essential in learning from an attack and helping to prevent any future incidents.

The essential elements for cyber resilience for your IR team

Whether your IR team is part of either your larger cybersecurity or IT team or working in a dedicated Security Operations Center (SOC), arming them with the right solution and strategy to be cyber resilient involves multiple moving parts.

Here are some essential elements for an incident response team to practice:

1 Preparedness and Planning:

Develop and regularly update an incident response plan that outlines roles, responsibilities, and procedures.

Conduct regular training sessions and simulations to ensure that team members are familiar with their roles and can effectively respond to different types of incidents. Ensure the IR teams are getting hands-on practice using the technologies and tools to do their jobs without the pressures of an incident.

2 Proactive Assessments:

Perform regular risk assessments to identify potential vulnerabilities and threats that could impact the organization.

Prioritize risks based on their potential impact and likelihood, guiding incident response efforts to address the most critical areas first.

Conduct regular compromise assessments and regular threat hunting to find previously undetected threats or identify threats earlier to enable proactive remediation.

3 Communication and Collaboration:

Establish clear communication channels within the incident response team and with other relevant stakeholders, and ensure these are documented in your plans and processes

Foster collaboration with external partners, such as law enforcement agencies, industry peers, and third-party incident response experts.

4 Continuous Monitoring:

Implement monitoring systems to detect unusual or suspicious activities in real-time. EDR, XDR, and SIEM are good starting points but have limitations when used in isolation. Integrating forensic-level visibility into the toolkit is essential for end-to-end investigation capabilities and improved outcomes.

5 Incident Detection and Analysis:

Develop and implement strategies for swift and accurate incident detection.

Invest in the right solutions that offer DFIR capabilities for complete analysis of incidents to understand the attack vectors, tactics, techniques, and procedures (TTPs) employed by adversaries.

6 Containment and Eradication:

Establish procedures for quickly containing and isolating compromised systems to prevent further spread of the incident.

Implement measures to eradicate the threat from affected systems and networks.

7 Recovery Planning:

Develop a comprehensive recovery plan to restore systems and services after an incident.

Establish backup and restoration procedures to minimize downtime and data loss.

8 Containment and Eradication:

Establish procedures for quickly containing and isolating compromised systems to prevent further spread of the incident.

Implement measures to eradicate the threat from affected systems and networks.

9 Recovery Planning:

Develop a comprehensive recovery plan to restore systems and services after an incident.

Establish backup and restoration procedures to minimize downtime and data loss.

10 Post-Incident Analysis and Learning:

Conduct a detailed post-incident analysis to identify lessons learned and areas for improvement.

Use insights from incidents to enhance the incident response plan, update security controls, and refine team processes.

11 Legal and Regulatory Compliance:

Stay informed about relevant legal and regulatory requirements related to incident response and data breaches.

Ensure that incident response practices align with legal obligations and privacy regulations.

12 Documentation and Reporting:

Maintain thorough documentation of incident response activities, including timelines, actions taken, and outcomes.

Generate incident reports for internal and external stakeholders, including management, legal, and regulatory bodies.

13 Adaptability and Continuous Improvement:

Stay abreast of the evolving threat landscape and adapt incident response strategies accordingly.

Continuously assess and improve incident response capabilities based on emerging threats and lessons learned from previous incidents.

By integrating these essential elements into their practices, incident response teams can enhance their cyber resilience, ensuring a more effective and coordinated response to cyber threats. This proactive and deliberate approach contributes to an organization's ability to withstand and recover from incidents, minimizing potential damage and disruption.

People, Process, and Technology – the pillars of cyber resilience in IR

People

Digital forensics requires specialists, contributing to the existing challenge of a cybersecurity talent shortage. But the security skills shortage also makes it hard to find and retain the right people with the right kinds of focus for this work.

That's where solutions and technology can help boost teams. Simplifying and elevating teams quickly can be achieved through collaboration, easy-to-use tools, and automation. Targeted training, drills, and using functional tabletop exercises are also important as they strengthen familiarity with different types of attacks and build muscle memory when it comes to responding to incidents.

Process

Security teams today rely on disparate tools, cross-functional communication, and sometimes fragmented methodologies that can threaten a consistent approach.

Having processes in place and a blue-print that guides responders through incident response helps to ensure rapid and coordinated action during security incidents to reduce response time and impact.

A well-architected and practiced incident response plan helps teams coordinate and navigate incidents with clarity while enabling the team with the adapted solutions can help to establish and standardize the approach for efficiency and seamless collaboration.

Technology

Many organizations turn to endpoint detection and response tools – both in their prevention efforts and for their IR needs. However, traditional Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Information and Event Management (SIEM) solutions have limitations when used in isolation.

Integrating forensic-level visibility into the toolkit is essential to ensure end-to-end investigation capabilities that go beyond containment and recovery. It's therefore imperative to review newer, next-gen solutions with DFIR capabilities that integrate with or augment existing security investments to bolster investigations and response through automation, collaboration, and speed. These offer a modern approach to the demands of contemporary incident response.

Binalyze helps you become cyber resilient

Learn how Binalyze can help progress your organization's journey toward cyber resilience by leveraging AIR, our Investigation and Response Automation Platform powered by DFIR.

Visit us at www.binalyze.com

Binalyze OÜ
Narva mnt 5, 10117 Tallinn
Estonia