Mattermost

Cybersecurity Incident Response Guide

The state of cybersecurity: Is your team ready for any incident?

Rapid digitalization of organizations from small businesses to massive public sector entities has generated a parallel need for cybersecurity strategies that can keep pace with next-generation cyber attacks and highly complex systems. The frequency and severity of global cyberattacks are on the rise, with hackers leveraging better technology to take advantage of the rapid rollout of online services that happened across many industries in the wake of the pandemic. Experts estimate that the cost of cybercrime will hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.

As the cost of cybersecurity incidents continues to increase, teams feel more pressure from customers and regulators to mature their own security practices. Whether they are large enterprises or small startups, companies fail or succeed by their ability to anticipate and respond to cybersecurity threats. For this reason, in a brief on a new National Cybersecurity Strategy initiative, the Biden administration called for greater investment in developing more secure and resilient software systems.

It isn't enough to be reactive to cybersecurity incidents when they happen. To ensure that they'll be able to resolve security threats and breaches efficiently and effectively, businesses must have a proactive cybersecurity strategy that enables them to respond to incidents quickly and collaboratively with established and trained procedures.

In this guide, we'll explore the cybersecurity challenges that businesses face today, look at how successful organizations apply best practices to ensure their teams are ready to act, and examine what you can look for when evaluating tools that will help your organization prepare for the threats ahead.

Key cybersecurity challenges

Cybersecurity is top of mind for businesses across the board, but what does that mean for the day-to-day priorities and processes of technical teams? Let's dig into some of the key cybersecurity challenges that organizations face and how they'll impact your team.

Smaller teams and budgets need to do more with less

After years of sustained growth, technology budgets are slowing down; Gartner revised their 2023 IT budget growth predictions down from 5.1% to 2.4% at the beginning of the year. Fortunately, most organizations still plan to prioritize cybersecurity budgets; security spend and risk management are forecasted to grow about 10% in 2023. However, security and operations teams may need to anticipate the need to do more with the team and tools they already have at their disposal. A survey of security professionals by the Ponemon Institute found that insufficient budget was the most commonly cited factor in preventing teams from working remotely without compromising security.

Cloud-native technologies give rise to new security concerns

Cloud-native technologies have found their place in enterprise tech stacks; as many as 94% of enterprises rely on cloud software to run their businesses. But while cloud technology has

great benefits in terms of speed, usability, and cost, it does have security implications.

Leveraging cloud-based infrastructure and tools can make cybersecurity more challenging, giving third parties access to some company data and limiting the control that security teams have over it. As a result, it can be harder to ensure that your organization maintains full data sovereignty and regulatory compliance when using cloud technologies.

How a secure collaboration platform helped a network of security pros share information and minimize the impact of an industry-wide breach

Cross-organizational information sharing and collaboration are essential to rapid response when major cybersecurity attacks occur, but cloud-based tools carry their own security risks. H-ISAC's global community of security professionals was reluctant to share sensitive data on other cloud collaboration platforms and instead relied on long email threads that were challenging to share and often lacked critical context.

Mattermost gave H-ISAC members a secure, self-hosted collaboration channel for information sharing and synthesis that let them respond effectively to cyberattacks, including NotPetya and Heartbleed, preventing catastrophic damage to their healthcare organizations.

Learn More

Complex software supply chains require additional security considerations

Modern software is complex, often leveraging artifacts from open source codebases and other third parties. But these components can introduce additional vulnerabilities to your software and increase risk of security breaches.

Gartner predicts that, by 2025, nearly half of global organizations will be impacted by supply chain attacks. The SolarWinds breach in 2020 cost the company at least $40 million — to say nothing of the cost to their clients. Monitoring the security of increasingly complex codebases requires a heavier lift from security teams; unfortunately, this task is more essential than ever.
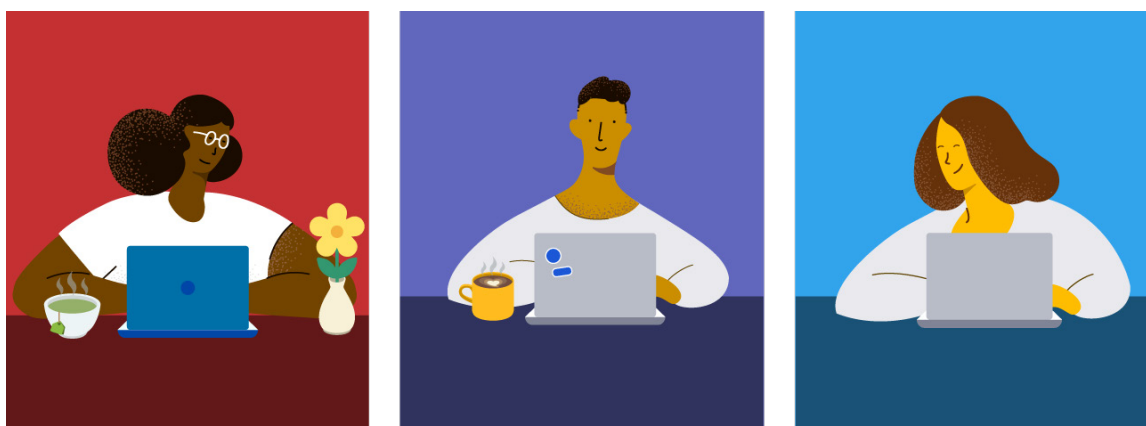
Remote and hybrid workforces require adaptable approaches to security

Cloud adoption isn't the only security threat teams must grapple with. Record numbers of mobile phishing attacks occurred in 2022, indicating that employees may be your organization's most vulnerable security vector. If your organization experiences a breach, the statistically most likely infection vector is still considered phishing, as the IBM X-Force Threat Intelligence Report reports. A greater reliance on home networks, personal devices, and mobile devices creates more endpoints that could introduce security concerns.

But it's important to note that while remote work is often cited as a security risk, where or how your employees work is not the main issue, as employees are targeted both on their personal and work accounts and devices. What matters is how educated they are about how breaches are conducted, how to identify attacks, and how they can request support from their internal security team.

Response to cyber incidents is slow, fragmented, and chaotic

While most teams would agree that cybersecurity is critical, many organizations aren't fully prepared for security breaches when they happen. In fact, one survey of security practitioners found that only 45% of technical organizations have an incident response plan in place to begin with.

When it comes to cybersecurity, every minute counts; outages and breaches can cost your organization tens or even hundreds of thousands of dollars per minute. IBM's study on the cost of data breaches found that in 2022, the average security breach took 277 days to identify and contain — and that the average U.S. business that was attacked paid $9.44 million to recover. Shortening your cyber incident response time can have a meaningful, measurable impact on your business — and your bottom line.

Best practices for cybersecurity incident response

For businesses of all sizes, security is no longer a nice-to-have; embedding strategic security practices in your technical and operational processes from the start is crucial to cybersecurity success. At the core of any cybersecurity strategy is a strong incident response plan. The more thorough and well-implemented your incident response plan, the better equipped your organization will be to respond to any cyber incident, large or small.

Let's dive into some of the best practices for creating and refining an impactful cybersecurity incident response plan.

Document and iterate your incident response planning

Many teams still use fairly ad hoc response playbooks when something goes wrong. Having a documented and tested incident response plan in place that your team can enact when an incident occurs allows them to respond effectively and ensure nothing slips through the cracks.

If you already have an incident response plan in place, what can you do to improve performance? Automating tasks and communication where possible can help your team move faster when minutes and even seconds count. Integrating your incident playbook into your

collaboration platform, rather than having it live in a separate document, can help your team put your plan into action more rapidly and evolve the process over time to respond to new threats in new environments.

Another great way to strengthen your incident response processes is to hold a retrospective after each run — whether for a real incident or a practice one — and use any insights gathered from your team to iterate and improve.

Read more:

Best Practices for Improving Incident Response Workflows

Want to improve your incident response plan? Focus on better incident communication.

The four critical components of effective incident management

Conduct tabletop exercises

No matter how thoroughly you plan for an incident, chances are that when your team must actually respond to one, you'll find something that could be improved. Practicing your response processes is one of the most effective ways to improve your response time and quality when the stakes are high. Tabletop exercises give your team a chance to run through their roles, procedures, and protocols, then address any weaknesses.

Keep in mind that tabletop exercises aren't just opportunities to rehearse your existing incident response processes; they can be a great way for your team to come up with novel approaches to solving problems that you might not have considered before, further strengthening your cybersecurity responses overall. Be sure to give stakeholders and participants space to react and respond after each exercise rather than just focusing on whether they stuck to the script closely.

Automate manual workflows

The manual tasks associated with any given process can be easy to dismiss as small enough not to matter. But when minutes and even seconds count, manual tasks like creating a Situation Room channel and populating it with the right people, cloning a task checklist, or even creating a Zoom call can add up. These tasks can slow down your team's workflows and distract them from actually identifying and resolving an incident.

Wherever possible, automating manual workflows will help your team stay focused and speed up their overall response time.

Read more:

An Intro to Designing Secure CI/CD Pipelines
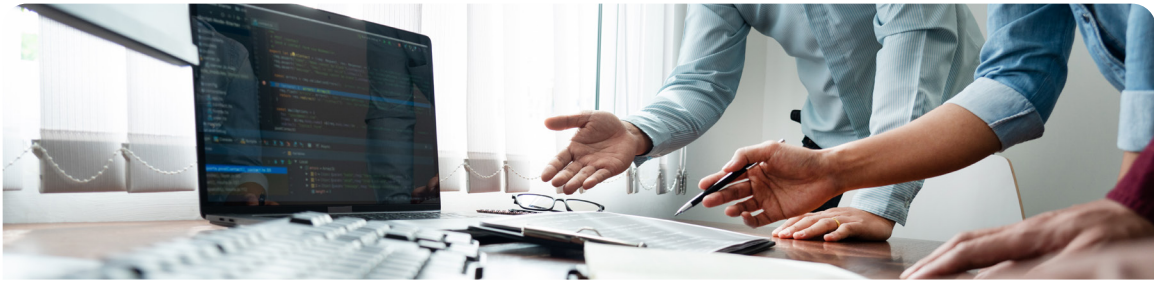
How automating reporting helps a top 3 bank improve MTTR by 90%

The IT team of a top-3 bank was working with a legacy chat system that didn't offer persistent chat and only supported disappearing, ephemeral group messaging. As a result, every new team member joining a response effort had to be manually briefed on the situation, which slowed down the process immensely with repetitive updates.

By introducing Mattermost, the bank was able to introduce automated reporting and smooth hand-offs across global time zones, ensuring that key stakeholders had the information and context they needed. Even more critically, the self-managed system met stringent compliance requirements for data control and action history archiving.

Learn More

Foster a strong security culture

Cutting-edge security tools and organizational processes don't matter if an employee falls victim to a phishing scam. According to Verizon's 2022 Data Breach Investigations Report, 82% of breaches involve a human element. As such, your first line of defense against security incidents is having a team that understands the importance of cybersecurity and knows how (and where) to report threats to the security team quickly to ensure fast response times.

Whether your team is in-office or remote, giving them access to tools that are easy to use and fit their needs plays a huge role in the adoption of secure tools and prevents data from leaking onto insecure channels. Practices such as enforcing multi-factor authentication, providing security training, and keeping sensitive information on controlled channels and devices all play a role in empowering your entire organization to play a positive role in your cybersecurity strategy.

Read more:

Tackling remote workforce security challenges post-pandemic

Have a business continuity plan in place

You have an incident response plan in place for when something goes wrong, but are you prepared for when something goes wrong with your incident response plan? Ensuring that you have a deep contingency plan in place for catastrophic "Sev0" outages and breaches is key. Such a plan should include establishing a backup channel for your communications on a system independent of your primary cloud infrastructure to ensure that first responders are never out of touch, no matter how widespread the incident may be.

Additionally, planning for less catastrophic but still significant deviations to your incident response plan can help your team execute their response more smoothly. For example, ensuring that every task has not just a designated owner but also a designated backup owner will prevent your response activities from being derailed by someone being out sick, on vacation, or otherwise unavailable.

How a global media company reduced costly outages by implementing a separate, secure collaboration platform for their DevSecOps team

For one global media giant lacking a Sev0 business continuity plan, the day finally came when a catastrophic outage knocked out an engineering division's infrastructure and communications. Over $100,000 of revenue was lost per minute of downtime, and the outage was drawn out because the team couldn't communicate without their regular systems.

Today, over 15,000 engineers at this global media organization use Mattermost for DevOps, digital operations, and business continuity on a platform completely separate from their primary infrastructure. They've moved away from IRC and Slack while maintaining Mattermost as their incident response home base with custom integrations to their own messaging systems.

Learn More

What to look for in an incident response collaboration platform

The right tools can enable your team to collaborate effectively before, during, and after a cybersecurity incident, helping accelerate time to resolution significantly. Look for these key features when evaluating incident response solutions.

⚙ Usability and core functionality

When an incident occurs, does your team know where to find and share the most up-to-date information? Your collaboration platform might be the best candidate for your incident response workflows. Keeping all of your tools in the same place and easily accessible by your team ensures that everyone can find the information they need quickly.

Keep in mind the kinds of information that your team and other parts of the organization will need to share as part of their incident response workflows. Evidence, process documentation, and remediation tracking are critical parts of incident response collaboration, so look for a solution that can support your team's work from end to end.

🔌 Robust integrations with essential tools

Tool and process overload can be a serious problem for security teams; Gartner reports that the average enterprise security team must manage around 76 security tools to keep their organization protected. Keeping track of the data going to and coming from those tools

can be overwhelming, so adopting a collaboration platform that allows you to integrate and customize your systems is key.

An incident response platform that is customizable and extensible allows your team and the greater organization to build integrations that are specific to your protocols and give actionable intelligence through persistent notifications. Additionally, by bringing notifications from your security and other technical tools together into a single platform, you'll give your organization better visibility into your security status while minimizing context switching.

🤖 Workflow and communication automation

Cyber incident response is a carefully orchestrated series of activities and communications, and every moment you spend on that process counts. Automating parts of your team's workflow wherever possible can help accelerate your response and keep your team focused on high-value tasks. Automation can also ensure that the right people are pulled into conversations early, avoiding the need to have all hands on deck all of the time.

Looking for incident response platforms that let you easily automate tasks for your team, from creating checklists with key response stages for a new incident to sending updates to stakeholders every hour during an event.

📒 High-availability architecture

An incident response system won't help if it's impacted by the same breach or outage as the rest of your infrastructure. Look for systems that offer high-availability environments to ensure that the platform is outage-proof and accessible no matter what. In addition, prioritize solutions that allow you to control your own data to ensure the maximum level of security over your recovery plan.

Why technical teams trust Mattermost for cybersecurity incident response

Mattermost helps security teams accelerate mission-critical work, even in the most complex environments, by allowing them to collaborate effectively and securely.

Increase organizational efficiency with a single collaboration hub
Mattermost's fast, familiar interface, collaborative playbooks, and customizable integrations let you create a workspace that slices through the noise to keep teams focused on high-impact workflows when minutes count.

Adapt your workspace to your workflow
Connect with in-house and SaaS-based tools with webhooks, plugins, API access, and source code access to customize Mattermost to fit your team's needs precisely. Legacy tools and proprietary software? No problem! With Mattermost's plugin framework you can connect those tools to Mattermost for easy access in mission-critical scenarios.

Stay in control with security-first deployment options
Maintain data control with a resilient collaboration hub that gives you the ability to deploy to any public or private cloud, including air-gapped networks. Conform to your organization's compliance and security standards without sacrificing usability.

"Playbooks supports emergencies really well. Communication on problems is transparent and open, and we're seeing much fewer requests by ticket or by phone."

— Jan-Peter Rusch, Software Architect and Developer   SCHÄFERBARTHOLD

Mattermost