The CEO's Guide to Cyberbreach Response

What to do before, during, and after a cyberbreach

AT&T Cybersecurity Insights | Volume 3

In **2015**, **62%** of organizations acknowledged they were **breached**.[1]

Yet **only** **34%** of organizations believe they have an **effective incident response plan**.[2]

Contents

For more information:

Follow us on Twitter @attbusiness

Visit us at

securityresourcecenter.att.com

Executive summary

With a nod to Tom Clancy, cyberattacks are a clear and present danger for every organization. Over one recent 12-month period, we logged more than 245,000 Distributed Denial of Service (DDoS) alerts across AT&T's global data network. More than 60% of businesses we surveyed had an IT security breach in 2015, and 42% of those organizations said a breach had a significant negative impact on the business.[3]

Organizations of all sizes and types face a growing variety of threats, from traditional brute-force DDoS attacks to more concealed — and usually more damaging — ransomware.

Most organizations have invested in a variety of tools, processes, and personnel to help protect sensitive systems and data against these threats. But given the sheer volume of attacks, it's highly likely that one or more will penetrate your defenses. This is why, in addition to threat prevention and detection, you must invest in a comprehensive incident response plan.

Successful incident response programs begin well before a breach occurs, and should be built as part of a broader business continuity strategy. Along with the tools and systems required to identify and respond to breaches, an incident response program requires two core components:

A cross-functional team. Because of the business implications of a successful cyberattack, post-breach response is often an all-hands-on-deck affair involving the C-suite, IT, security, legal, communications, and other teams across the organization. AT&T and other service and technology partners also play a role, as do law enforcement agencies, regulators, and, of course, customers.

Frequent testing. Just as your organization holds regular crisis management exercises for various scenarios, an incident response plan must be regularly tested so that all involved parties are crystal clear about their respective roles and responsibilities. These roles must be reinforced through regular tabletop testing and other simulations. The goal is to eliminate the guesswork and uncertainty that can arise in a potentially chaotic situation.

This up-front work will let you respond quickly after a successful attack. The first 24 hours are obviously critical to contain the breach and limit its impact. This is where forensic investigation comes into play. Not only is it needed to discern the nature and extent of the breach, forensics is instrumental in containing the incident.

If the breach requires public disclosure, you'll also need to soothe the concerns of customers, address media queries, and meet with regulators and law enforcement — activities that can linger for months, depending on the scope of the breach.

Let's be clear: Incident response can make or break your business. Some companies have tallied losses in the tens and even hundreds of millions of dollars after suffering severe breaches. In those cases, the CEO, CIO, or other executives may ultimately take the fall. This report, based on our internal practices, our Global Cybersecurity Readiness survey, and the work we've done with customers, is intended to help you avoid that doomsday scenario.

The first 24 hours

- **Activate your incident response plan**
- **Remove or isolate the infection**
- **Assess legal implications**
- **Determine root cause**
- **Define critical business impact**

Preparing for the inevitable

In this section:

62% of organizations acknowledged they were breached in 2015 alone.[4]

Only 16% of passive companies have a strong incident response plan in place.[5]

Bottom line: The inevitability of a cyberbreach, and its potential impact on your business, requires an up-to-date, effective incident response program.

Breaches often occur under the most mundane of circumstances. A trusted employee stops by a restaurant after work and while he dines, his work laptop is stolen from his car. Now imagine the possible result: the organization is brought to a complete stop after the thieves access the laptop, steal passwords, and access the business's IT systems.

In this scenario, the first hint of an issue isn't until the company's servers go down, with employees unable to access any files or emails. The short-staffed IT team is slow

How ready are you? Four types of organizations

The AT&T/IDC Global Cybersecurity Readiness survey identifies four levels of security preparedness:

Progressive. This is the highest level of security readiness, in which C-level executives pay close attention to security and invest in a holistic, comprehensive prevention and response strategy.

Proactive. Companies with above-average levels of security readiness realize the importance of IT security and have put in place basic steps to avoid breaches.

Reactive. At companies with below-average levels of security readiness, C-level executives pay moderate-to-little attention to security while delegating security expertise and day-to-day management to IT.

Passive. The least-prepared organizations are run by executives who take a hands-off stance. They tend to be unaware of most breaches and reactive in response to breaches they do detect.

to react, and by the time external forensic specialists are called in to help minimize the damage, it's already too late. Critical data is lost, records have been stolen, and the business was unable to function. The cost of one vulnerable laptop to the organization quickly escalates to hundreds of thousands of dollars as the organization moves to repair systems and plug security vulnerabilities.

This story is increasingly possible as hackers up their game and organizations struggle to keep up. For example, in the public sector, nearly three-quarters of state legislators and staff believe their state's level of cyberrisk is moderate to high, according to an AT&T/National Cybersecurity Alliance study. Despite the risk, 80% of respondents don't know if their state has an emergency plan in place to respond to a breach.[6]

The lesson from this hypothetical company's painful story is not just that a breach took place. No, the lesson here is that they were completely unprepared to quickly address the breach — because they lacked a clear plan to respond.

The importance of incident response

The ongoing digitization of business operations and data is helping companies to become more flexible, responsive, and innovative. But

digital transformation is also increasing the vulnerability of sensitive data and systems to cyberattacks.

The threats are numerous and diverse. Many, such as DDoS attacks, have been around for years but have begun to scale as the methods and tools become available to the masses. Over one recent 12-month period, for example, AT&T logged more than 245,000 DDoS-related alerts across its global data network.

Other threats, such as emerging strains of ransomware, are more recent — and potentially more damaging (see "What happens if your data is held hostage?," page 15).

More business and IT leaders are accepting the grim reality that one of these attacks will be successful. Sixty-two percent of cybersecurity professionals believe their organization is likely to suffer a successful attack in the year ahead — a sharp rise from just two years ago, when 38% said they were likely to be breached.[7]

Given the "when, not if" mindset that now permeates the cybersecurity market, executive teams need to be proactive in their approach to mitigating successful cyberattacks. That's where a sophisticated incident response program comes into play.

By clearly spelling out the participants, processes, and lines of reporting following a serious cyberbreach, an incident response plan goes a long way toward mitigating the impact of a breach. The Global Cybersecurity Readiness survey finds that 74% of the best-prepared organizations have a sophisticated and comprehensive program in place that assesses their breach response capabilities and includes a clear plan for diagnosis, response, forensics, and remediation.

Unfortunately, simply developing an incident response program does not mean that your organization will respond swiftly and effectively to a breach. While 81% of companies have an incident response plan in place, just 34% consider those plans to be effective.[8]

245,000

AT&T logged more than 245,000 DDoS alerts over a recent 12-month period

Too often, the costs and complexities associated with incident response planning and preparation may cause some companies to shortchange these activities. Among organizations that don't have an incident response plan in place, 40% cite a lack of

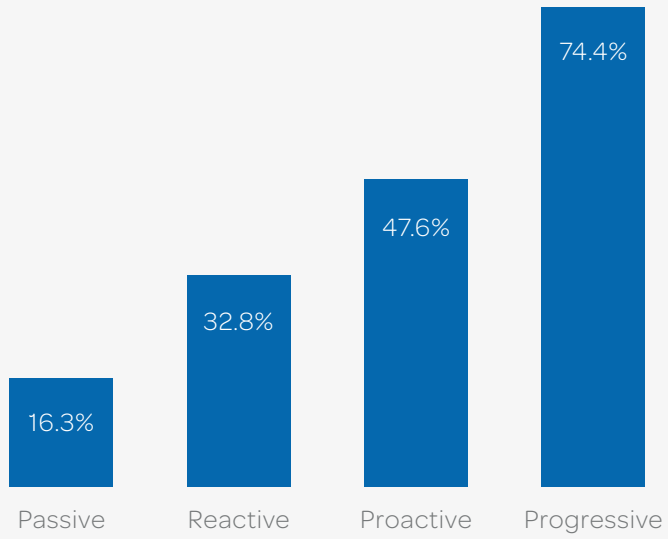
Know the term:

Ransomware

A type of malware that restricts access to data and demands that a payment be made to the attacker to restore access

Progressive companies are better prepared for a breach

% of companies that have a strong incident response plan that includes regular tabletop exercises and breach diagnosis



Incident response plan: Core components

1. Define all breach scenarios and their specific response steps
2. Outline preventative measures
3. Define stakeholders, roles, and responsibilities
4. Create internal and external communications templates
5. Specify response priorities
6. Maintain business continuity

Know the term:

Tabletop exercise

A meeting to discuss a simulated emergency situation

resources or budget as the reason.[9] In other instances, companies that are focused on speeding time to market and driving innovation may — by design or default — simply avoid tackling tough incident response demands.

"A thorough and well-understood incident response plan helps minimize the duration and impact of security events," says Michael Klepper, national practice director for Security Consulting Services at AT&T. "Like many things in life, you get out of it what you put into it."

In our hypothetical scenario, had the organization been better prepared, it would have had proper controls in place to prevent the theft of a stolen laptop from opening the door to significant system damage. It also would have had an incident response plan in place to see to it that a breach can be quickly contained. Regular tabletop exercises could have given agency employees practical experience in reacting more quickly to an insider breach. All of these steps could have prevented the loss of data — and the workplace disruptions that followed.

A cyberbreach is no time to find out you're unprepared. As our hypothetical company learned too late, an up-front investment in incident response quickly pays for itself when a breach does occur.

What does a progressive company look like?

The progressive organization represents the highest level of cybersecurity maturity in the AT&T/IDC Global Cybersecurity Readiness survey. These organizations share several key qualities that help them rise to the top.

Pragmatic: C-level executives at progressive companies understand they are targets of breaches. That mindset enables them to take a more pragmatic approach to incident planning and response. For example, many progressive companies use technologies to sharply reduce the value of compromised data to hackers.

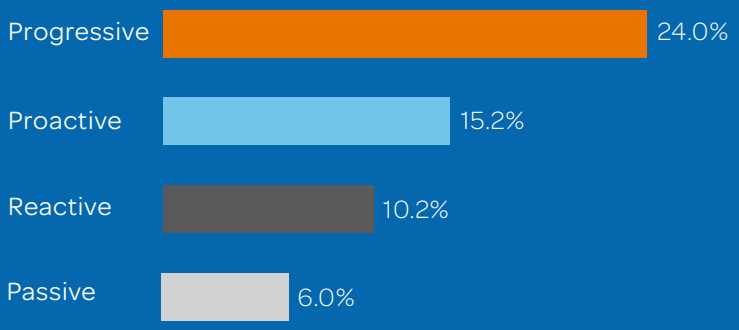
Comprehensive: Progressive companies are more likely to focus as much on readiness assessments and diagnosis planning as they do on post-breach diagnosis and response (74% for progressive organizations versus 16% of passive companies).

Diligent: Progressive companies perform near-constant security reviews and use third-party service providers to supplement the bandwidth of their internal security teams. Sixty percent of progressive companies say their senior executives require daily security status updates, versus 14% of passive organizations.

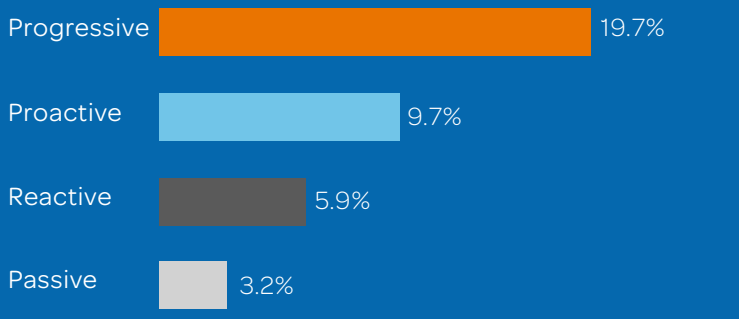
Successful: The companies with the highest levels of IT security readiness also exhibit better business outcomes. Progressive companies averaged 24% sales growth over the past three years compared to 6% for passive organizations; their profit margin grew by 20% compared to 3% for passive companies; and their customer satisfaction increased 22% compared to 2% for passive companies.

In other words, being security-ready is good for business.

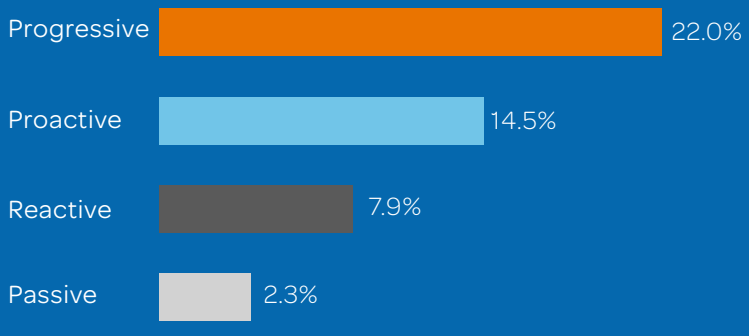
Progressive companies have seen greater 3-year growth in revenue ...



... profits ...



... and customer satisfaction.



Source: AT&T/IDC Global Cybersecurity Readiness, 2016

Before the breach: The best offense is a good defense

In this section:

Incident response requires the formation of cross-company plans and teams with every stakeholder department represented.

Only 9% of companies update their incident response plan at least twice a year.[10]

Bottom line: The ability to quickly mitigate the effects of a breach requires a strategic, dynamic, fully tested incident response plan.

Successful incident response programs begin well before a breach occurs. We're not suggesting, however, that response planning trumps defensive measures such as intrusion prevention and detection. As we underscored in our first Cybersecurity Insights report, organizations must be proactive in setting up a strong line of defense to mitigate cyberrisk.

Tools such as automated threat response systems are increasingly critical for speeding threat identification, isolation, and resolution activities. Such tools form an important bridge between threat prevention and incident response.

"The last thing executives want is to be informed by law enforcement or another third party that their data has been leaked," says Bindu Sundaresan, practice lead for Security Consulting Services at AT&T. "That's where a sophisticated incident response program comes into play."

Beyond putting the tools and systems in place to identify and respond to attacks, an incident response program requires two other core components: a cross-functional team and frequent testing.

Putting the team together

Building an incident response team is no simple task, as it should include representatives from a broad array of stakeholders, including the C-suite, IT, information security, legal, compliance, and public relations, among others. The members of these cross-functional teams play various but equally vital roles in developing the incident response plan and the written incident response playbook.

A company's legal team and its compliance officers, for example, can provide critical counsel on privacy laws, federal and industry regulations, and other requirements that could come into consideration after systems or data are compromised. Legal can also help create templates for post-breach legal notifications or programs to redress any parties injured by the breach.

Often, the CSO will serve as the primary team leader and coordinator. However, the CEO must be a visible and vocal proponent to help

Incident response team structure

Stakeholder	*Roles and responsibilities*
CEO/Senior leadership	• Empowers people who provide support for initiatives to help reduce risk and mitigate the effects of an incident • Helps protect intellectual property, customer data, and compliance with data security regulations
IT/Security	• Determines the cause and the extent of the damage • Analyzes and interprets logs • Leads forensic evaluations • Coordinates recovery efforts and internal communication • Preserves evidence
Legal	• Provides legal guidance • Reviews press statements • Contact for outside legal representation or law enforcement
Communications	• Drafts press statements • Contact for the media and the public • Assesses potential public reaction in response to a security incident
External organizations (as needed)	• Provide expert help in incident response and forensics • Liaise with management on legal, regulatory, and service issues

A key factor in rapid analysis

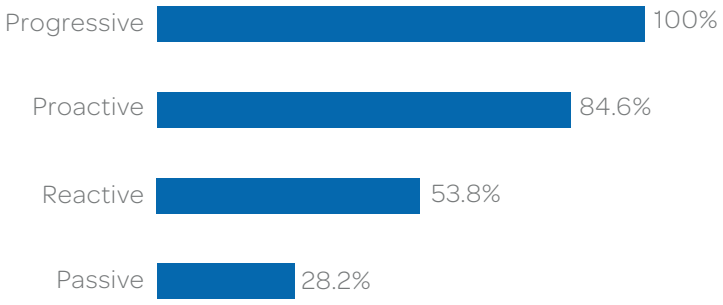
When a breach occurs, it must be quickly identified and contained, which may mean taking some infected or suspect systems offline or isolating specific network segments. Putting the right security management and tracking tools in place ahead of successful attacks is critical to the rapid analysis and mitigation of those breaches, and the investigation of how they occurred.

Companies in heavily regulated industries, such as health care, already have stringent requirements for collecting and retaining log data. But log data is critically important for any organization that suffers a security breach, because it helps forensic experts perform post-breach investigations.

Despite the value this log data holds, forensic consultants at AT&T often find that it doesn't exist when customers call them in to help diagnose and mitigate successful cyberattacks.

"We consistently go in and find that the evidence data we need just isn't there or readily accessible," says Todd Waskelis, executive director of Security Consulting Services at AT&T. "This makes it difficult for us as we try to figure out what happened."

Forensic tools are a must-have for progressive companies



Source: AT&T/IDC Global Cybersecurity Readiness, 2016

facilitate the creation of incident response plans and teams and to back them with the authority they require.

External stakeholders also play a critical role in incident response planning because they can bolster your response skills and capabilities. Among others, those outside partners can include law firms, cyberinsurance companies, computer forensic consultants, service providers, communications professionals, crisis management specialists, and law enforcement agencies.

CEOs need to assess the strengths and weaknesses of their in-house incident response team and supplement it as necessary with outside experts — before a breach occurs. Companies that wait until they're in post-breach fire-drill mode to seek outside help have likely already fallen behind in their response. It's much more effective to develop relationships with strategic partners before their services are required.

Many companies, in fact, place critical strategic partners on retainer to confirm their availability and rapid response should a cyberbreach occur. These partners can provide tools and expertise to assist with complex yet critical tasks such as forensics. Investing in forensic tools is particularly important, not just for identifying the cause of a breach, but also for helping to thwart future attacks (see "A key factor in rapid analysis"). Every progressive

Part of a healthy routine

In this new world of cyberbreaches, organizations are often surprised when their incident response plans fail to deliver. Consider the all too possible scenario of an employee at a health plan provider falling for a phishing email scam. The results could be devastating for the organization as well as the clients, with the potential loss of highly sensitive health records and social security numbers. Without a practiced, effective incident response plan, an organization could quickly find itself vulnerable and unprepared.

Minimizing the damage from a phishing scam or similar breach requires regular tabletop exercises to rehearse potential scenarios and an up-to-date response playbook that accommodates advances in the field, such as electronic medical records for health care companies.

While every response plan is unique, a robust tabletop exercise should answer these questions:

- Has the breach been contained?
- Have the affected systems been isolated?

- Who will lead forensic evaluations?
- Was company or customer data exposed?
- How many records were accessed?
- Have regulators been notified?
- Will the public be notified?
- What is our post-breach messaging?

Regularly reviewing and practicing your incident response plan is vital to the success of your overall cybersecurity plan. Otherwise, you won't know what you don't know until a crisis hits.

organization in the AT&T Global Cybersecurity Readiness survey has invested in forensic tools, compared with just 28% of passive companies.

Education and testing

Having a written incident response plan and a cross-departmental team in place is of little value unless all involved parties are crystal clear about their respective roles and responsibilities — and how they're expected to work with other team members. These roles should be reinforced through regular testing and simulations. The goal is to eliminate the guesswork and uncertainty that can arise in a potentially chaotic situation.

Know the term:

Cyberinsurance

A liability policy that insures against damage from cybercrime

The most common form of an incident response test is the tabletop exercise. Tabletop tests can help team members meet to practice their roles in a variety of different scenarios. Through these scenarios, the team can gain greater familiarity with incident response workflows and communications. The tests can also help reveal any flaws or gaps in the incident response plan and processes.

What's in your incident response playbook?

Get a quick, effective, and orderly response to security breaches with a thorough and regularly tested incident response playbook. AT&T recommends including the following incident management scenarios and procedures.

Scenarios to include	*Procedures to include*
• DDoS attacks • Theft of customer information • Theft of employee information • Theft of intellectual property • Ransomware, malware, viruses • Social engineering of personnel	• Contact incident response team • Escalate to senior leadership • Comply with regulatory or industry reporting obligations • Notify employees, customers, business partners, investors, media, law enforcement • Isolate and mitigate causes of the breach • Prevent recurrence of the breach

Members of the leadership team — up to and even including the CEO in some cases — should participate in the portions of the tabletop practice sessions that involve reporting structures, executive decision-making, and external communications. Even if every exercise doesn't demand executive leadership's direct participation, they still must stay informed about the results and authorize improvements when the tests identify areas of incident response weakness.

Tabletop exercises should also incorporate real-world events. For example, the team can use small-scale incidents that were easily contained as practice for larger events. Ask questions such as: What if the incident was bigger or went further? What if we didn't find it? What if a team member wasn't available when the incident occurred?

"It's important to work with real-world scenarios," says Todd Waskelis, executive director of Security Consulting Services at AT&T. "If someone from the media calls, how is that handled? Are they routed to the authorized PR contacts? You're trying to gauge how well people understand the plan, how well they're working together under pressure, and where the gaps are that need to be reinforced."

"You're trying to gauge how well people understand the plan and where the gaps are that need to be reinforced."

Todd Waskelis
Executive Director
Security Consulting Services
AT&T

Tabletop exercises are critical, but they also have their limits, at least from a technical response perspective. IT and security teams can take their incident response planning a step further with more realistic tests such as simulation exercises and full-scale testing, during which one or more systems are shut down and brought back up at an alternate site. Often, these exercises are done as part of a broader business continuity program.

"CEOs must make sure that cybersecurity and incident response are part of their business continuity and disaster recovery planning,"

says Mike Paradise, vice president of Global Operations and Infrastructure Services at AT&T. "Companies may have to shut down critical systems, move operations to backup sites, and do all they can to minimize downtime and its associated costs."

Tabletop and other exercises should be conducted regularly — at least twice a year, if not quarterly. An incident response plan will get stale if it sits on the shelf. Just as business models and cyberthreats continually evolve, so must incident response plans and preparations.

In this area, there's plenty of room for improvement, because companies clearly are not doing enough. Fewer than 10% of organizations in one recent study review their incident response plans two or more times a year.[11] More than one-third said they had not reviewed or updated their incident response plans since they were initially developed. Another 36% said they have no time period set for reviewing and updating their plans.

Barring direct experience with a serious cyberbreach, too many companies are prone to let incident response remain a back-burner issue. In doing so, however, CEOs are playing a high-stakes game of security poker in which the odds ultimately favor the cyberattacker.

"Preparation is the key to all of this," says Brian Rexroad, executive director for Technology Security at AT&T. "When you learn of a potential breach, it should not be the first time you're thinking about a response. You need to hit the ground running."

You also need to be flexible. No matter how well prepared you may be, no matter how many different scenarios you lay out, assume that something unexpected will come up at some point and you'll need to improvise to some extent.

What happens if your data is held hostage?

Ransomware is just what it sounds like: an attack in which criminals hold data assets hostage until the victimized organization pays a fee. Companies must pay the ransom to receive a file decryption key or free up their locked computers. And ransomware's threat to business is rising. Researchers tracked more than 4 million samples of ransomware in the second quarter of 2015, up from 1.5 million just two years earlier.[12]

So what should you do if hackers slip past your defenses? As with any ransom situation, there's risk that even if you pay, the criminals will continue to extort the business.

If you are unable to remove the virus, your immediate responses should be:

- Disconnect the infected system from the network
- Restore compromised data from backups
- Evaluate how long the affected systems can be offline before your business is affected
- Decide if forensic experts have time to counter the attack
- Notify law enforcement

Considering the cost of downtime in dollars, ransomware response is a necessary — but complex — addition to any incident response playbook.

After the breach: Rapid response

In this section:

Knowing how to appropriately react for a range of breach types can save time, money, and your company's reputation.

Bottom line: Poorly coordinated incident response activities may cause more damage than the breach itself.

The email arrived shortly after the payment processing company's website began experiencing slowdowns. The chilling message: You're being attacked, and the attacks will worsen until you pay a digital ransom in bitcoins.

The company, which processes $37 billion annually in transactions, could not afford any downtime. Nor could it simply pay the ransom, since there were no guarantees that the attackers would stop after the first payment. So the company's leadership and security teams quickly sprang into action. They first contacted the FBI, which confirmed that the threat was

real. Then they called their service provider to help them analyze and address the threat.

Within two hours, a mitigation plan was in place. Two hours after that, a defender program was launched against the DDoS attack to protect the at-risk systems.

The extortionists kept their promise to launch future attacks — but the reinforced defenses repelled the attacks "like they were bouncing off titanium," the firm's chief marketing officer said. The attack was resolved with no payment to the criminals — and no downtime for the payment processor's mission-critical website.

This example shows how the preplanning that goes into an incident response program enables an organization to move quickly to identify the scope of an incident and then take decisive steps to mitigate the damage.

Post-breach activities fall into two main categories: early-stage mitigation and post-containment analysis and communication.

Early-stage incident response activities

No two cyberattacks or data breaches are identical, nor are the ways in which companies first become aware that something's wrong. Small attacks or probes may be automatically detected and countered, or quickly contained by a company's security team. The seriousness of a breach may be immediately apparent, or its scope and damage may only emerge over time. But whether a major breach is only suspected or actually confirmed, the company's incident response plan comes into play.

Even at the first hint of a breach, the playbook should define a clear process for identifying a potential threat and prioritizing next steps. Consider building a set of tiered responses that are triggered by the escalating nature and severity of the threat. If a high-impact breach is confirmed, the CEO, board, and other key players must be quickly brought into the loop. Full incident response plans, processes, and teams go into effect when the breach is deemed serious enough to require full IT forensics and remediation, along with regulatory, legal, and public disclosures. These types of activities and programs can last for months, if not years.

Your team's commitment to adhere to the playbook is instrumental throughout a breach. In sports, if one team member decides to play by their own rules, the chances of winning are generally slim. Fully committing to the incident response playbook requires confidence that your plan — and team — will succeed.

Your security team will almost always lead the early incident response charge, given the imperative to identify the nature of the breach. This team will then work closely with the IT department to contain its spread and to terminate its activity. For small- and medium-size businesses, the security team and the IT department could have the same personnel, making their involvement in incident response planning even more critical.

Service providers may play a critical role as well. Last spring, students in Texas used a DDoS attack to shut down their school district's system four days before standardized testing was set to begin. The attack shut down the ability to take attendance, distribute grades, and assign tests or homework. A prolonged outage would have crippled the district.

Fortunately, network administrators detected the attack after just five minutes; within 15 minutes of confirming the attack, they began diverting the targeted IP address through specially designed "scrubbing complexes" to mitigate the attack. Minutes after the traffic was passed through the scrubbers, the attack was controlled. By the end of the school day,

Know the terms:

Security incident
Unauthorized access to assets, such as data, networks, and devices

Forensics
Collects, analyzes, and reports on data to use in the detection and prevention of a breach

traffic levels were back to normal and the issue was successfully resolved.

This example speaks to the importance of having a plan to rapidly isolate compromised systems when a breach is confirmed, while also firing up backup systems to minimize downtime. Although some of these actions may be automated, others require IT personnel to evaluate the situation before responding.

Security teams and other incident response team members may have to perform rapid risk analyses, some of which will require C-suite involvement in the decision process. The CEO may be asked to weigh the damage an infected system might cause against the costs of shutting down critical systems and operations for hours or even days. These decisions aren't made lightly: Enterprises experienced an average of 23 hours of downtime as a result of security incidents in 2015, while small- and medium-size businesses averaged nearly 14 hours of downtime.[13] For some organizations such as ecommerce vendors, even an hour or two of downtime can translate into millions in lost revenue.

As security and IT teams work to contain and mitigate a breach, other actions and communications are activated. Relevant information about the breach needs to be distributed internally to C-suite executives, legal and compliance departments, the corporate communications team, and any impacted business units.

During this initial breach identification and containment period, it's important to assess when (or whether) to disclose the breach outside of the company. While affected

customers or business partners will need to be informed quickly, going public with news of the breach may require more time. When your team is still working to counter and assess the scope of the breach, public attention can cause unnecessary confusion and concern, both internally and externally. Plus, any incorrect information that you release can be difficult to correct or clarify later.

Companies have learned this lesson the hard way. In late 2013, one day after a security website reported that Target was investigating a large data breach, Target CEO Gregg Steinhafel confirmed that data was stolen and said the breach affected 40 million customers. In the weeks following the breach, Target was forced to repeatedly revise its initial estimate, eventually settling on its final tally of 70 million. The inaccurate claims fed a storyline of mismanagement — and ultimately contributed to Steinhafel's resignation.

Post-crisis responsibilities and actions

Once a breach has been contained and business operations have been restored, some of the most challenging work and communications gets underway. Security and IT teams — often with the assistance of outside experts — must perform computer forensics and other postmortem tasks to fully understand the root cause of the breach and confirm that that the threat has been eradicated. As noted earlier, having the right tools in place up front tremendously improves the accuracy and detail of this work.

"The knowledge gained from threat forensics and analysis will shore up organizations' cyberdefenses," says Alex Cherones, director of product marketing for Threat Management Solutions at AT&T. "It's a vital step in preventing successful future attacks."

As IT teams work through their forensics, mitigation, and remediation tasks, they will collaborate closely with corporate lawyers and compliance officers. Among other tasks, these departments will coordinate with federal and state law enforcement agencies to help identify the people, organizations, or countries behind the breach. At the same time, the legal and compliance offices will assess their organization's own liability for any exposed personal information or compromised laws and regulations.

The applicable laws and regulations can vary greatly depending on the nature of the breach, the industry sector in which a company operates, the geographies in which it does business, and many other factors. Often companies are obligated to promptly notify law enforcement groups, federal agencies, and others of the breach. Preapproved notification templates and distribution lists will help an organization quickly comply with any such requirements. The same goes for any contractual obligations that require notification of partners, customers, or others after a breach.

Beyond legal and regulatory communications, a victimized company will also field questions

"The knowledge gained from threat forensics and analysis will shore up organizations' cyberdefenses. It's a vital step in preventing successful future attacks."

Alex Cherones
Director, Product Marketing
Threat Management Solutions
AT&T

Navigating breach communications

When it comes to post-crisis messaging, there are a number of best practices to follow:

- Respond quickly, but resist the instinct to overcommunicate
- Rely on boilerplate statements that have been prepared in advance and preapproved by stakeholders
- Focus on customers in your public messaging, and not so much on your company
- Consider setting up a section of your website where customers, the press, and others can get up-to-date information about the cyberbreach and your company's response to it
- Promote a proactive message about the positive steps your company is taking in response to the breach

from customers and the media. An incident response plan should clearly spell out who will serve as the primary public spokesperson(s) and enforce strict message discipline and flow. For major breaches, the CEO often serves as the lead public spokesperson to deliver messages about how the breach occurred, how future breaches will be prevented, and what the company will do to support and compensate customers or any other injured parties.

In the wake of the massive Sony hack in November 2014, Sony made several missteps in its public communications. Initially, the company released a vague statement about investigating an "IT matter," then characterized the breach as a "system disruption." As the hackers leaked more and more information, executives were put on the defensive about the sensitive content being released. Sony's outside counsel sent cease-and-desist letters to the media in an attempt to keep them from publishing the leaked documents — a tactic that was viewed as desperate and defensive. In an attempt to contain its scope, Sony took far too long to acknowledge the breach and focus on how it was fixing the problem.

One overriding communications strategy is to focus less on the damage to your company and more on the steps you're taking to protect your customers. Consider setting up a website where customers, the press, and other interested parties can get up-to-date information about the breach and your company's response to it. That's one tactic Home Depot took in 2014 after discovering that customer debit and credit card information had been breached. The retailer quickly set up a website to keep customers informed about the breach and ways to protect their personal information.

A communications plan that focuses on helping the customer rather than describing the problem also has a side benefit: limiting media interest.

Conclusion: Your call to action

Preparing for and defending against a cyberattack has been a priority of security and IT professionals for some time. But many organizations are underprepared for reacting to an actual breach.

Incident response is so multifaceted — and so critical — that CEOs must play a leadership role in driving comprehensive response programs across their organizations. They should make incident response an investment and operational priority to see to it that any damages caused by a major breach are kept to a minimum.

We've seen firsthand the damage that can occur when organizations don't react quickly and decisively to a breach. We've also witnessed how organizations that are well prepared can limit the short- and long-term damage of a successful cyberattack.

The cyberthreat landscape is constantly evolving. But our data shows that the majority of threats are well known and easily defended — if you have the right controls and planning in place. A tailored incident response plan, with a core cross-functional team, is an integral part of this preparation.

Our experience working with customers and protecting our own global network has given us insight into a playbook for incident response, which we have shared with you. Our research has shown that organizations that are more proactive about cybersecurity exhibit higher levels of profits, growth, and customer satisfaction.

Preparation is the key to a robust breach response. To ensure that your organization can react quickly and limit damage you should:

- **Invest in prevention and detection technologies to defend against day-to-day attacks**
- **Build a response team that includes all key internal stakeholders, from the C-suite to first responders**
- **Have a clear plan for the first 24 hours after breach detection**
- **Conduct regular tabletop exercises**
- **Establish protocols with your service providers on breach response**

It's impossible to predict when you'll be hit by a cyberbreach. The ability to respond quickly and thoroughly will determine whether the breach becomes a minor footnote or a major distraction that inhibits company growth for years to come.

Additional reading

- Cybersecurity Insights, vol. 1: What Every CEO Needs to Know About Cybersecurity
  www.corp.att.com/cybersecurity/archives/v1
- Cybersecurity Insights, vol. 2: The CEO's Guide to Securing the Internet of Things
  www.corp.att.com/cybersecurity/archives/v2
- Executive Abstracts
  www.corp.att.com/cybersecurity/abstracts
- Know the Terms glossary
  www.corp.att.com/cybersecurity/terms
- Network Security Solutions
  www.business.att.com/enterprise/Portfolio/network-security
- More resources available at
  securityresourcecenter.att.com

Endnotes and sources

1. AT&T/IDC, Global Cybersecurity Readiness, 2016
2. Experian/Ponemon, Is Your Company Ready for a Big Data Breach?, 2015, http://www.experian.com/assets/data-breach/white-papers/2015-experian-data-breach-preparedness-study-final.pdf
3. AT&T/IDC, Global Cybersecurity Readiness
4. ibid
5. ibid
6. AT&T/National Cybersecurity Alliance, Cybersecurity Survey of State Legislators and Staff, 2016
7. CyberEdge Group, Cyberthreat Defense Report 2016, http://www.cyber-edge.com/2016-cdr/
8. Experian/Ponemon, Is Your Company Ready for a Big Data Breach?
9. ibid
10. ibid
11. ibid
12. Norton, S. (2015, Nov. 10). 'Ransomware' Attacks to Grow in 2016, Says Intel's McAfee Labs [Web blog post]. http://blogs.wsj.com/cio/2015/11/10/ransomware-attacks-to-grow-in-2016-says-intels-mcafee-labs/
13. PwC/CSO, Global State of Information Security Survey 2016, 2015

"Sound cybersecurity practice equals preparation and rapid response for garden-variety attacks as well as emerging threats — either of which can cause major damage."

Jason Porter
Vice President
Security Solutions
AT&T

MOBILIZING
YOUR
WORLD℠

att.com/cybersecurity-insights