The CEO’s Guide to Cyberbreach Response

Executive Abstract | AT&T Cybersecurity Insights | Volume 3

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.

“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,” says Brian Rexroad, executive director for Technology Security at AT&T.

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, executives may ultimately take the fall. The CEO’s Guide to Cyberbreach Response is based on our internal practices, our Global Cybersecurity Readiness survey, and the work we’ve done with customers, and is intended to help you avoid that scenario.

Most organizations have invested in a variety of tools, processes, and personnel to help protect 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 you must invest also in a strong incident response plan.

“Sound cybersecurity practice equals preparation and rapid response for garden-variety attacks as well as emerging threats — either of which can cause major damage,” says Jason Porter, vice president for Security Solutions at AT&T.

Breaches happen. But most companies aren’t prepared

62%

of organizations acknowledge they were breached in 2015

Yet only

34%

of organizations believe they have an effective incident response plan

Sources: AT&T/IDC, Global Cybersecurity Readiness, 2016
Experian/Ponemon, Is Your Company Ready for a Big Data Breach?, 2015

The first 24 hours

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

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.

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
- 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

Prepare for the inevitable

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.

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.

Before the breach: The best offense is a good defense

Successful incident response programs begin well before an attack occurs, with a strong intrusion prevention and detection program. But an incident response program requires two other core components: a cross-functional team and frequent testing.

Incident response team structure

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

Building an incident response team is no simple task, as it should include representatives from a broad array of stakeholders, such as the C-suite, IT, information security, legal, compliance, and public relations.

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. Regular tabletop exercises and simulations will reinforce these roles — and eliminate the guesswork and uncertainty that can arise in a potentially chaotic situation.

After the breach: When rapid response matters

Even at the first hint of a breach, your playbook should define a clear process for identifying an escalating potential threat. Full incident response plans, processes, and teams come into play when the team deems a breach serious enough to require full IT forensics and remediation, along with regulatory, legal, and public disclosures.

"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."

42%

of organizations said a breach had a significant negative impact on the business

Source: AT&T/IDC, Global Cybersecurity Readiness

Navigating cyberbreach communications

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

- Respond quickly, but resist the instinct to over communicate
- 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
- Promote a proactive message about the positive steps your company is taking

Preparation is key to robust breach response

Incident response is so multifaceted – and so critical – that CEOs must play a leadership role in driving comprehensive response programs across their organizations.

To ensure that your organization can react quickly and limit damage you should:

Invest in prevention and detection technologies. Protecting your organization against day-to-day attacks is the first layer in a complete cybersecurity plan.

Build a response team that includes all key internal stakeholders. Because of the business implications of a cyberattack, post-breach response is often an all-hands-on-deck affair, from the C-suite to first responders.

Have a clear plan for the first 24 hours after breach detection. Critical to containing the breach and limiting its impact is your ability to react confidently and appropriately within the first 24 hours.

Conduct regular tabletop exercises. A plan is of little value unless all involved parties are clear about their roles and responsibilities.

Establish protocols with your service providers on breach response. External stakeholders play a critical role in incident response planning because they can bolster your response skills and capabilities.

MOBILIZING
YOUR
WORLD℠

Download the full report at att.com/cybersecurity-insights