AVERTIUM®

eBook

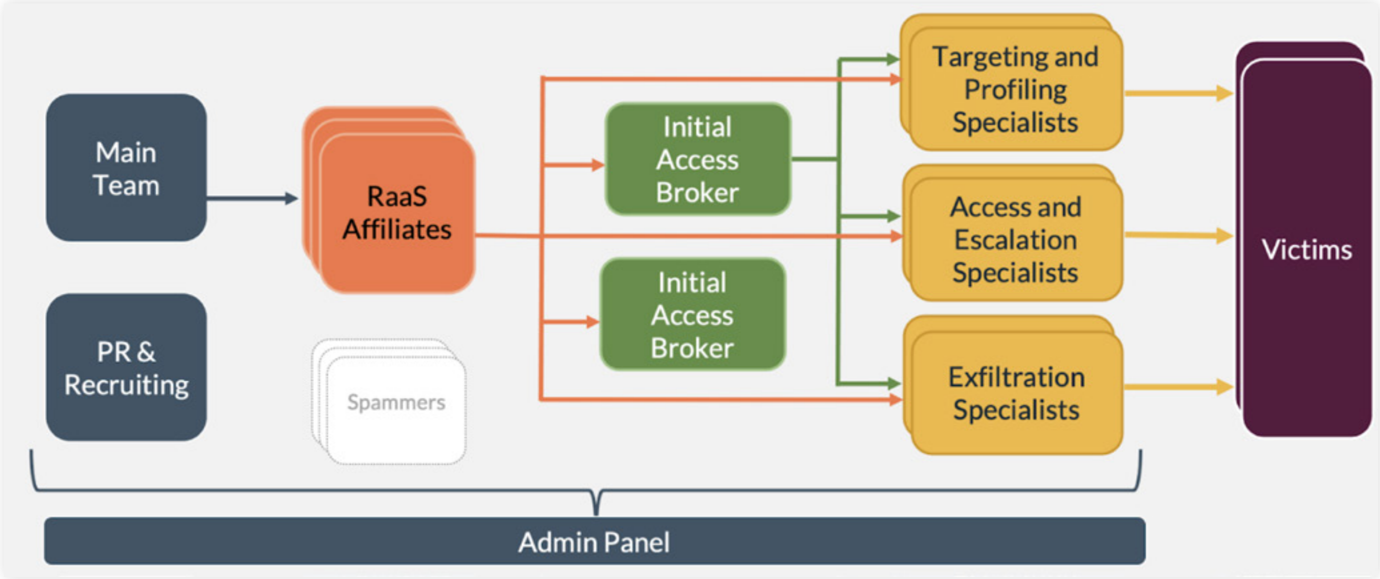
# CREATING A BUSINESS-FIRST INCIDENT RESPONSE PLAN

# TABLE OF CONTENTS

# INTRODUCTION

Recovering from a breach is easier said than done. The historical attitude about breaches from most companies has been "it won't happen to us." In the last couple of years, however, companies have changed their tune… but leadership still might not quite understand the full scope of the damage that could be done by a breach or ransomware attack.

The typical data breach is electronic in nature, a bad actor gaining access to resources through one vector or another. Once this is accomplished, they have access to a treasure trove of sensitive corporate information. It could be a system where cardholder data is processed, stored, and maintained corporate IP in the form of upcoming product plans and releases, or servers where HR data resides. Any or all of this can create valuable cash streams for the hacker today. A breach can come through a variety of channels within your attack surface and entails more than just lost data — it has ramifications for every aspect of your organization and, in some cases, can lead to the end of a business.

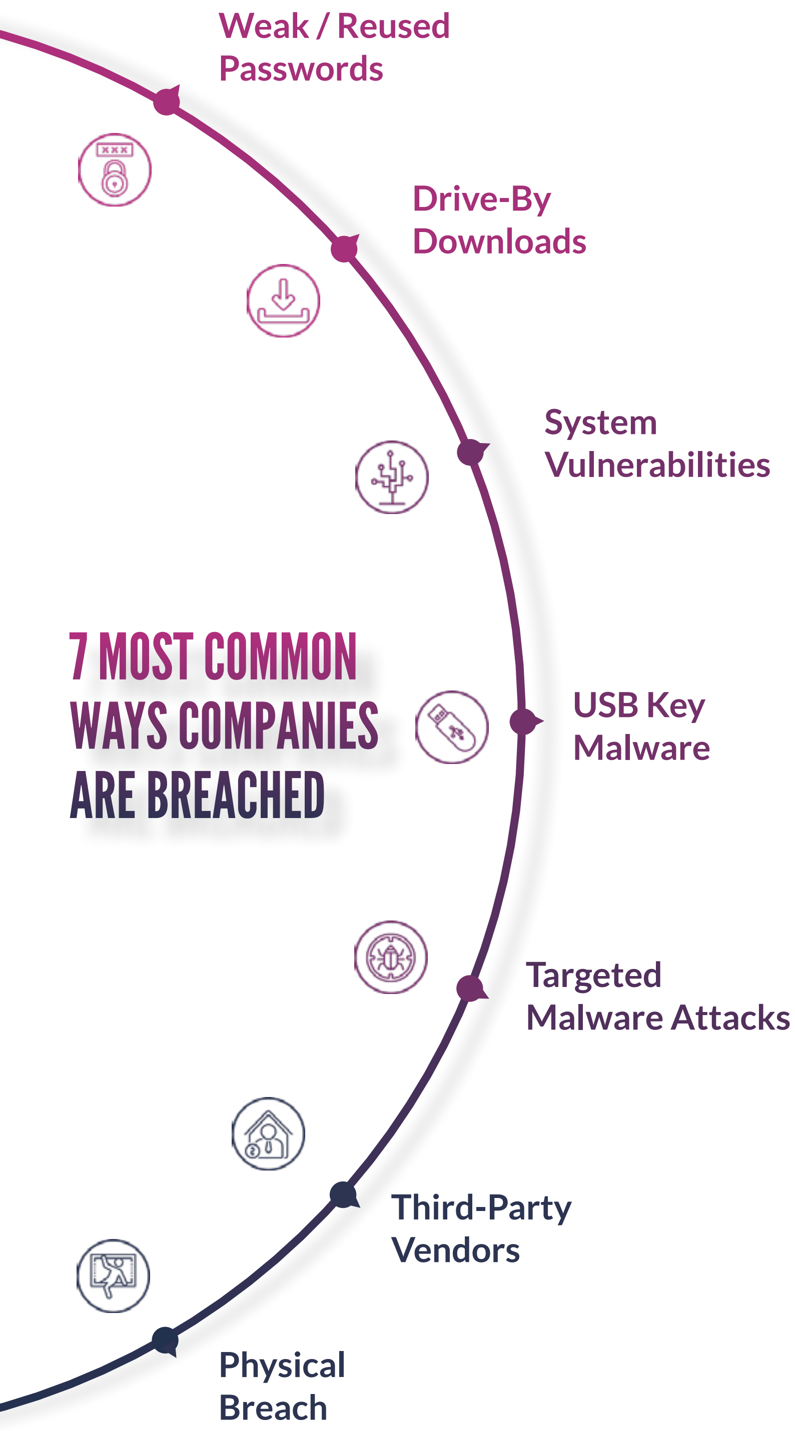


*Cybercriminals are operating at increasingly new levels of sophistication. They now look more like a SaaS enterprises and less like a group of ragtag criminals.*

**Related Content:**

1. *8 Steps to Take if You've Been Breached*
2. *You're Secure - But are Your Vendors? Assessing Third Party Risk*

According to Norton, these infiltrations can originate from a number of different sources. **To name a few of the most common ways companies are breached:**



## 1. Weak / Reused Passwords

Password cracking software can be used to recover passwords that have been forgotten. These applications make use of different methods for recovering passwords — common methods include the Dictionary Attack, Brute Force Attack, Rainbow Table Attack, Cryptanalysis, and simply guessing the password. As computing power has increased, so has the ability to crack passwords with lightning speed.

Hackers often use these same tools / applications that can guess passwords in a matter of seconds. Just because your users' passwords are "complicated" doesn't mean hackers can't get in. If hackers find a user's password on a third-party site, they will immediately try it for other, more valuable accounts.

## 2. Drive-by Downloads

A drive-by download attack occurs when malicious malware is unintentionally downloaded to your computer or mobile device, leaving you vulnerable to a cyberattack.

These attacks, unlike many other types of cyberattacks, do not require the user to actively "allow" the attack — you don't have to click on anything, download anything, or even open a malicious email attachment to become infected. Drive-by downloads can take advantage of a security hole in an app, operating system, or web browser that has been left unpatched due to failed or omitted upgrades.

## 3. System Vulnerabilities

One of the most prevalent causes of incidents is system vulnerabilities. Once a software or system vulnerability is discovered, attackers target companies who leverage it, using the vulnerability as an entry point.

To name a few system vulnerabilities that attackers commonly target:

- **Remote Desktop Protocol** (the most common)
- **VPN Appliance Vulnerabilities** (i.e. Fortinet and Pulse Secure)
- **Privilege Escalation Vulnerabilities**
- **Outdated / Unpatched Software**
- **Zero Day Vulnerabilities**
- **Noncompliant + Unsupported Legacy Servers** (i.e. Windows 2008 or 2012)

## 4. USB Key Malware

Any USB / jump drive can contain infected files. In some cases, these are purposefully left laying around in inconspicuous places, so people will think they've come into a windfall of a free USB drive. But once the drive is plugged in, the malware contained on the drive now lives in that device.

## 5. Targeted Malware Attacks

Attackers can and will use all forms of malware attacks — from phishing emails, to attachments, to even toxic links within emails — to deploy malicious software on a computer.

## 6. Third-Party Vendors

Your company might have strong security protocols, but your vendors may not. Your vendors and other third-party members are an extension of your organization, and therefore they are also entryways for ransomware.

## 7. Physical Breach

This is when there is an actual physical theft of equipment. Think laptop theft from a car, or sensitive documents that can be taken when someone tailgates through the main security checkpoint. Also think of the items that could be at risk as an intruder roams your interior space. Though it's true that most important documents are kept online nowadays, there are still piles of paper documents. If an intruder were to wander through a cube farm, they're bound to see important paper within in/outboxes and on desks.

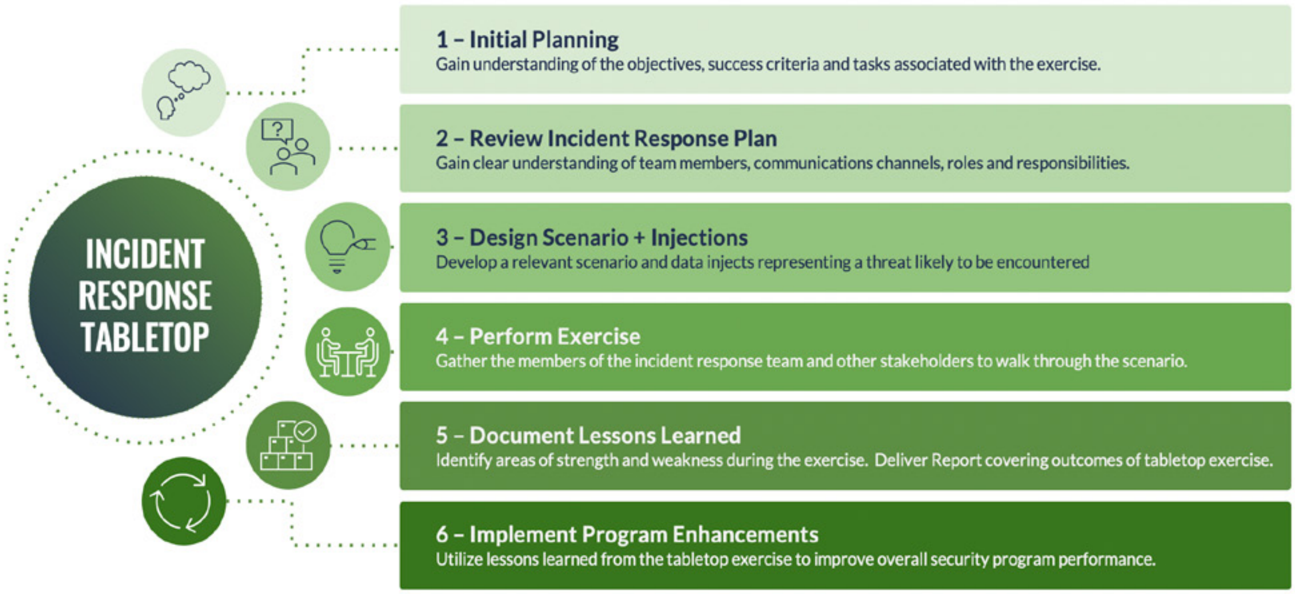
# IR PLAN PART 1 – PREPARING FOR THE INCIDENT

Preparing for an incident begins with an incident response (IR) plan. A traditional IR plan is a document that outlines an organization's procedures, steps, and responsibilities of its IR program. It begins with preparation, moves through incident response, and ends with recovery. How each business handles these crucial time periods will be the determining factor in whether their organization will survive the breach at hand.

That said, each organization's IR plan will look different. Cybersecurity consultancies like Avertium can help your business understand and mitigate the risk of a breach by performing cybersecurity assessments that identify areas of vulnerabilities, assess your cybersecurity resiliency, and analyze the potential business impact that could result from a breach.

**Here is a list of what a typical incident response plan includes:**

- How IR supports the organization's broader mission
- The organization's approach to IR
- Activities required in each phase of IR
- Roles and responsibilities for completing IR activities
- Metrics to capture the effectiveness of its IR capabilities
- Communication pathways between the IR team and the rest of the organization



INCIDENT RESPONSE TABLETOP

**1 – Initial Planning**
Gain understanding of the objectives, success criteria and tasks associated with the exercise.

**2 – Review Incident Response Plan**
Gain clear understanding of team members, communications channels, roles and responsibilities.

**3 – Design Scenario + Injections**
Develop a relevant scenario and data injects representing a threat likely to be encountered

**4 – Perform Exercise**
Gather the members of the incident response team and other stakeholders to walk through the scenario.

**5 – Document Lessons Learned**
Identify areas of strength and weakness during the exercise. Deliver Report covering outcomes of tabletop exercise.

**6 – Implement Program Enhancements**
Utilize lessons learned from the tabletop exercise to improve overall security program performance.

# TIPS for Incident Response Preparation

## TIP 1. Create an internal crisis team composed of more than just cybersecurity professionals.

When responding to an incident, let's not confuse speed with haste. Creating an internal crisis team that's made up of stakeholders from PR / marketing, legal, leadership, finance, and cybersecurity ensures that when a crisis strikes, your company has the ability, the agility, and the accountability structures in place to mobilize as fast as possible while also remaining as strategic as possible.

## TIP 2. Enlist the right external partners PRIOR to the incident.

Just like it is important to enlist the right internal stakeholders, it's also very important to know the experts that you can turn to in the event of a breach. When responding to an incident, time is of the essence. Therefore, enlisting the right partners prior to an incident prevents your company from losing precious time on contracts and approvals when an incident actually happens.

**The teams you need:**

1. Legal / Counsel Breach Coach
2. Digital Forensives + Incident Response (DFIR)
3. Public Relations (PR)
4. Cyber Insurance

### LEGAL / COUNSEL BREACH COACH

Enlisting a legal partner that knows the ins and outs of cybersecurity and breaches might make sense in the event that your business has questions about notifying the public, compliance implications, or faces litigation associated with the breach.

### DIGITAL FORENSICS + INCIDENT RESPONSE (DFIR) TEAM

From a technical standpoint, you'll want to have a Digital Forensics and Incident Response (DFIR) Team at the ready to investigate and contain the breach, and, in the case of a ransomware attack, potentially communicate and negotiate with the attacker.

According to BMC, here are some of the capabilities you can expect from a **DFIR service solution**:

- **Data acquisition** that **spans** a number of sources, multiple devices, and systems
- **System transparency** that offers **clear visibility** into actions and administrative processes
- **Investigation capabilities** that are **comprehensive and compliant**
- **Reporting** including **features** like robust visualization
- **Automating iterative processes** that help incident managers find all instances of artifacts, faster, with less guesswork

### PUBLIC RELATIONS (PR) TEAM

If you do not have a public relations (PR) team internally, you'll want to form a relationship with an external PR or reputation management firm to ensure that you can approach the media narrative around the breach with tact and minimize the reputational loss that comes from the breach.

You can expect the following from a PR / Crisis Comms Team:

- Develop **template communications** like press statements
- Help you **navigate internal communications**
- Help you **navigate external / media communications**
- Liaise with **legal counsel**

### CYBER INSURANCE

Cyber insurance, also known as cyber-liability insurance, is an insurance policy that helps protect organizations from the fallout of cyberattacks. There are two categories of financial protection in cyber insurance, first-party and third-party:

1. **First-party cyber liability insurance**
   - **What it is:** It assists in your organization's internal financial recovery after a breach as well as getting your own network and systems back in order.
   - **Who it's for:** This insurance is best for anyone who utilizes technology throughout their company and digitally stores any data.
2. **Third-party cyber liability insurance**
   - **What it is:** It provides financial help in the event that clients, customers, and partners affected by the cyberattack on your network are now pressing charges against your organization.
   - **Who it's for:** This insurance is best for any company that holds, transfers, or has access to sensitive customer data. Breaches that encroach on client information are likely to face more litigation from outside parties.

## TIP 3. Get the tools and processes in place for incident prevention and threat detection.

When it comes to a breach, **the best offense is a good defense**, which means getting the right tools and processes in place to detect and mitigate the risk of a breach from happening in the first place.

### DETECT + CONTAIN USING TECHNOLOGY

- EDR / Anti-Malware — Endpoint Detection and Response is a platform of automated tools and capabilities that continuously monitor a system for suspicious activity within the security perimeter.
- Security Information + Event Management (SIEM) — Collect data from all corners of your digital environment. The correlation will help identify suspicious events that may be uncommon to your team. It is hard to identify when there is an issue within your cyberspace if you don't have a clear vision of what it'd normally look like.

- Zero Trust Network (ZTN) — Close any possible vulnerabilities your organization may have. This goes along with monitoring your third-parties and limiting what access they may have to your data and cybersphere.
- Email Protection — Each member in your company is a channel for ransomware users to take advantage of... and emails are an easy bait for them to use. DMARC, DKIM, and Microsoft 365 capabilities are all ways to combat spoofing. Using these tools in conjunction with an email gateway to strip malicious email content can help safeguard your emails and decrease the size of your attack surface.

### MITIGATE RISK BY UNDERSTANDING THE HUMAN ELEMENT

- **Third-Party Risk** — Your vendors and third-party members are an extension of your organization and therefore they are also entryways for ransomware. Adjust your supply chain to ensure that each party you interact with understands cybersecurity and incorporates it into their own digital landscape. Learn more about third-party risk assessment.
- **Behavioral Analysis** — Signatures are unreliable. That's why it's important to detect malicious activity through analysis of the network AND user behavior. Then, you can get a clearer picture and investigate the true anomalies.
- **Threat Intelligence** — Power up detection with enriched data about known threats, indicators of compromise, and tools to enable threat hunting.

  *Check out these free resources you can incorporate into your daily feed:*

  » The Spamhaus Project — A European non-profit organization that tracks cyber threats and provides real-time threat intelligence.

  » Department of Homeland Security (DHS): CISA Automated Indicator Sharing — Intelligence sharing service allows for private companies to report cyber threat indicators to the DHS, which are then distributed using the automated indicator sharing website.

  » FBI: InfraGard — Portal managed by the FBI and provides information to 16 sectors of critical infrastructure.

  » SANS: Internet Storm Center — The SANS Institute is one of the most well-respected information security training institutes.

## TIP 4. Preserve business continuity by backing up your data often.

Ransomware targets company data and holds it hostage. Therefore, one way to take the wind out of an attacker's sails is by having data backup performed very regularly.

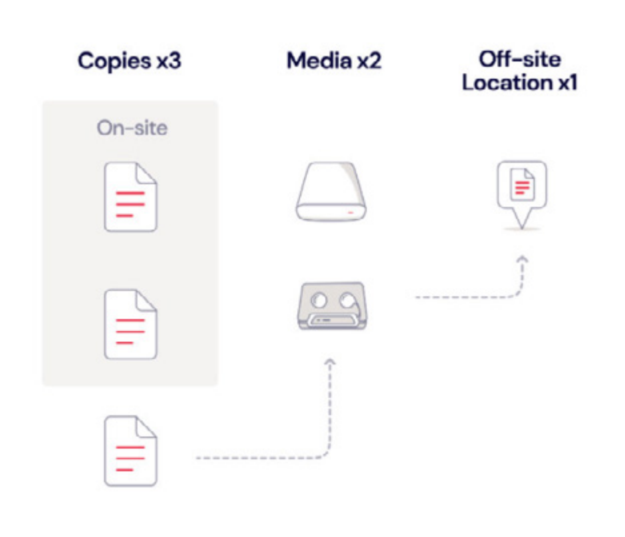
**Related Content:**

1. *New Techniques to Strengthening Threat Detection and Response*
2. *Leveraging Zero Trust Architecture to Contain & Combat Ransomware*

But let's be clear: the term "backing up" does not just refer to making sure you have your most recent information stored. It means having multiple locations for your data, utilizing different storage formats, AND always making sure it is up-to-date.

Typically, companies fall into one of these categories:

1. **They have a backup plan, but don't test it:** This leads to problems when they need to access backups and they can't access the data in the format needed.
2. **They don't back up their systems regularly enough:** Out-of-date backups lead to data loss.
3. **They don't protect their backup systems adequately:** When you're breached, you don't immediately know which data was accessed when, what was compromised, or where the breach spread to. Having offline backups is absolutely critical to ensure your backups don't become another victim of the breach.



## **TIP 5.** Put your IR plan to the test.

There are different ways of testing your business' IR plan, but each is necessary in finding your organization's vulnerabilities and giving insight into how things will go in case of an attack. Remember to continue testing your IR plan each time your information is updated and adapted to new digital environments to ensure bad actors never get the upper hand over your organization.

### 3 WAYS TO TEST + PREPARE

1. **Red Team / Blue Team Exercises** — This is an exercise where "red teams" test the effectiveness of a security plan. These teams emulate the behaviors and techniques of likely attackers, designed to be as realistic as possible. The "blue team" is the internal security team that is charged with stopping these simulated attacks. The aim of these exercises is to test an organization's security maturity as well as its ability to detect and respond to an attack.
2. **Tabletop Sessions** — In a tabletop exercise, your team meets to discuss their roles during an emergency and their response to a security breach. Your company CISO or a director for your IR plan will take the group through different scenarios, allowing you to think practically through the role and response of your security response team.
3. **End-User Training Sessions on Detecting and Reporting Suspicious Activity** — Data security is a team effort. Your end-users are your first line of defense against malicious attacks. Communicate regularly with your team so that even the most non-technical among us can identify when something looks suspicious.

SUMMARY OF TIPS

## IR Plan Part 1 — Incident Response Preparation:

1. Create an internal crisis team composed of more than just cybersecurity professionals.
2. Enlist the right external partners PRIOR to the incident.
3. Get the tools and processes in place for incident prevention and threat detection.
4. Preserve business continuity by backing up your data often.
5. Put your IR plan to the test.

# IR PLAN PART 2 – DATA BREACH RESPONSE AND RECOVERY

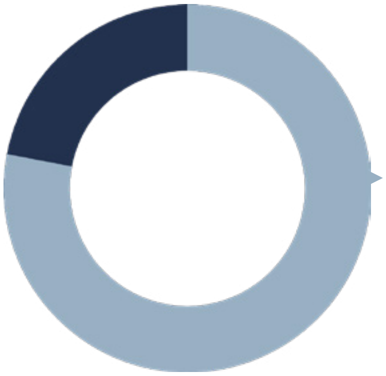
When a crisis strikes, a company's response can have a major impact on the damage done.

**Considerable costs to the company include:**

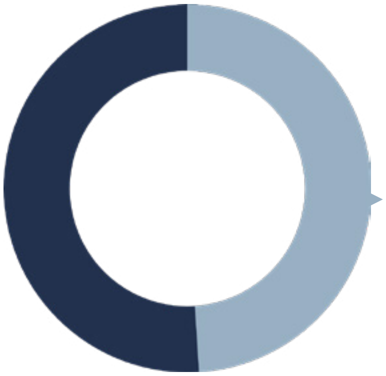
1. Initiating response protocols
2. Launching an investigation
3. Engaging forensic professionals
4. Assessing + containing + remediating the attack
5. Declining revenue due to customer and partner confidence

Future costs such as fines and lawsuits may also impact the costs of breaches. Fines are levied for insufficient technical and organizational measures to ensure security. Not to mention, there is also a significant increase in the number and complexity of data breach lawsuits - many of the recent class-action lawsuits for data breach have claimed negligence, failure to exercise reasonable care, and failure to protect sensitive client and employee data.

A survey by Ping Identity found that a **single data breach** can cause:



78% of consumers disengage with your brand



49% would not sign up or acquire a product / service from a company that recently reported a data breach

**Related Content:**

1. *T-Mobile Data Breach Review: 40 Million Customers Compromised*
2. *TIR – 20210920 T-Mobile and BlackBerry - Why Waiting to Inform May Cost You*
3. *Navigating Cybersecurity & Managing Data Breach Risks*

# TIPS for Your Response and Recovery

## TIP 1. Mobilize internal resources strategically.

When a breach occurs, clarity around what comes next is imperative. Having an internal crisis team ready to deploy can help to ensure that your team is ready and equipped to respond, but it's also important that every employee in the company remains a united front amidst the upcoming media scrutiny. This requires clear guidelines on the do's and don'ts of how employees should be discussing the incident externally.

## TIP 2. Have a clear communications strategy.

It's not possible to control the media, but you are able to limit and control the resources of information you give to them about your organization. There are a few ways to combat the reputational loss associated with a breach:

### OFFER ANSWERS THAT ARE ACCESSIBLE AND TIMELY

The last thing anyone wants in a breach is people jumping to conclusions due to a lack of information. That's why it's important to answer common questions and address concerns from customers and partners via easily accessible channels. Have an announcement banner on your website, deploy emails to your customer list, use any and all channels you have at your disposal to tackle the issue head-on.

In a recent data breach involving T-Mobile, the company released a webpage entitled "The Cyberattack Against T-Mobile and Our Customers: What happened, and what we are doing about it," which keeps their customers updated on what is occurring internally. In addition, they made sure to stay active and open in their communications to the public. Having created a webpage for both affected customers and updated news on the situation, they were able to establish that they cared about keeping their customers and the public informed with each step they took.

### HAVE A UNIFIED MESSAGE TO THE MEDIA

Once you establish the comms strategy, use negative media coverage to your advantage. Speak publicly about it and maintain as much consistency as possible, emphasizing the action steps your company is taking to address customer data loss or exposure and how you'll prevent future attacks.

### MONITOR AND RESPOND TO SOCIAL MEDIA MENTIONS

It's also important to monitor and respond to social media during a PR crisis. This can help plan for future communication plans, correct any misinformation or misconceptions about the breach, and show your customers and prospects that your company is taking the incident seriously. Your marketing team can use resources such as mention.com to keep track of where you are being talked about, how you're being talked about, and your brand sentiment over time.

## TIP 3. Learn and grow from the incident.

Whether it is a full-blown breach or just a phishing attempt, an investigation should follow each and every security incident. With this information, you are able to optimize your cybersecurity infrastructure and prevent attacks in the future.

**What to take from a breach:**

### ROOT CAUSE

Investigating a breach or disturbance is the first step in order to know exactly what happened and where your security fell short.

### ADDRESS THE ROOT CAUSE

Don't just let the cause of the event be noted. Go through and analyze how it was able to happen and notify your team so they're able to notice these issues, as well as, understand what can happen if these issues go unnoticed.

### STAY UP-TO-DATE

Revisit your IR Plan and update it with what you learned through this process and enable tools and processes that are suited to eliminate these issues from reoccurring.

It's vital to change with the times or else your plan won't be effective. New systems have to be identified, prioritized, and integrated into the plan. In doing so, your IR Team will always be up-to-date and prepared following a potential incident.

SUMMARY OF TIPS

## IR Plan Part 2 — Your Response and Recovery:

1. Mobilize internal resources strategically.
2. Have a clear communications strategy.
3. Learn and grow from the incident.

**Related Content:**

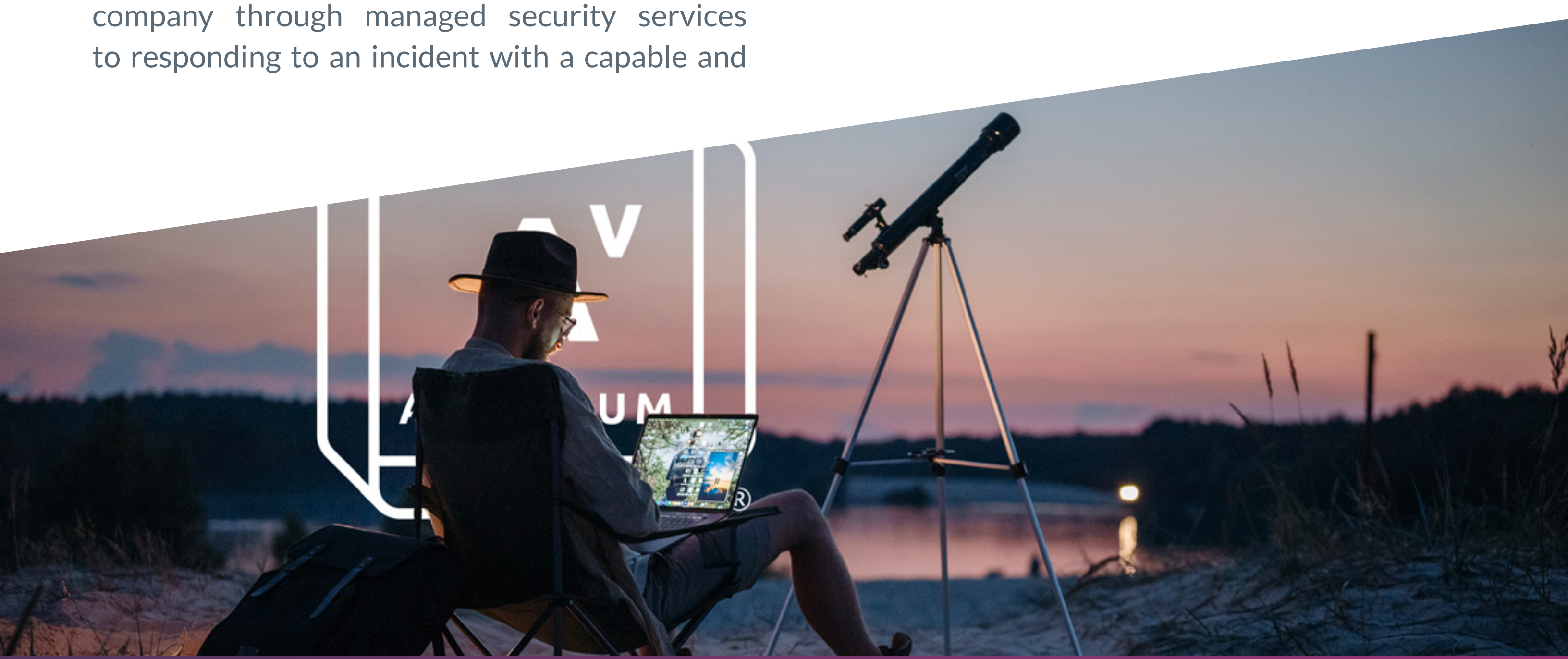
1. *Why Root Cause Analysis is Crucial to Incident Response (IR)*

# NEED HELP UPDATING YOUR INCIDENT RESPONSE PLAN?

An IR plan is **not a process that can be templatized and distributed** to any company. **To fully protect your business and respond quickly** in case of crisis requires a plan that is developed around your unique company, its risk profile, and the threat landscape.

Avertium can help your company **at every stage of the incident response lifecycle** — from assessing your risk, crafting a business-first incident response plan, and protecting your company through managed security services to responding to an incident with a capable and competent DFIR team. Our solutions are **custom-built for your IT environment**.

In conclusion, **attacks can come from anywhere** — your customers, your workforce, your partners, or of course, overall bad actors. No business is immune from cyberattacks. Everything you can do to improve your security posture, such as no-password methods and Zero Trust-Networking, helps keep you from being another statistic.



**Don't let your organization fall to a preventable attack.**

Learn more on how you can advocate for cybersecurity in our latest eBook:
*"Why the Time is Now for CISOS to Advocate for Cybersecurity (and How to Do It)"*

# | ABOUT AVERTIUM

**Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context.** By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why **over 1,200** mid-market and enterprise-level organizations **across 15 industries** turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

## CONNECT WITH US

AVERTIUM

**Cyber Fusion Centers of Excellence**
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

This publication contains general information only and Avertium is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Avertium shall not be responsible for any loss sustained by any person who relies on this publication.

SHOW NO WEAKNESS®