Building a better Incident Response Plan

INTERNETWORK ENGINEERING

cisco

Gold Partner

An Incident Response Plan is a critical component of your overall security strategy

You're probably leveraging anti-virus software, endpoint monitoring, or firewalls to protect your users and data – but do you have a detailed, documented plan in place for when you actually experience a security incident? With the risk of an attack or data breach higher than it's ever been, having an Incident Response Plan in place is absolutely critical:

The rising number of security incidents

According to real-time tracking, 5.1 million data records are being stolen on a daily basis, and almost 4,000 are stolen every minute.[1]

Threats are getting harder to detect

Only 49% of IT professionals strongly believe their organization can detect security weaknesses before they become real incidents.[2]

Malware is becoming more vicious

Cybercriminals are creating malware that can evade the traditional detection methods (like sandboxing) upon which many organizations rely.[2]

Ransomware will only worsen

Estimated ransomware damage costs saw a 15X increase from 2015 to 2017, and are expected to grow exponentially as cybercriminals target more organizations.[3]

What's even more unsettling is that it takes the average organization 100 to 200 days to discover a security incident in the first place.[2] At the end of the day, if you aren't thinking about the security threats you face and preparing for what could happen, it's impossible to expect that your organization will continue to operate at its best.

In this eBook, we'll share a few best practices and provide some tips on building or strengthening your organization's Incident Response Plan.

SOURCES: [1]Real-time Data Breach Statistics at breachlevelindex.com, [2]Cisco's 2016, 2017 and 2018 Annual Cybersecurity Reports, [3]CSO Online from IDG, Top 5 Cybersecurity Facts, Figures, and Stats for 2018

The components of a strong Incident Response Plan

In many organizations, response to security incidents is handled on a case-by-case basis, and often in direct response to a breach. This approach may work for common occurrences like low-level malware or compliance issues, but ransomware attacks and large-scale breaches require more strategic planning, consistent processes, as well as continuous detection and monitoring – all parts of a strong Incident Response Plan.

Recommended components of your Incident Response Plan:

Threat detection

The first step in responding to security threats is effectively detecting them in the first place:

- IT or security teams should be up-to-date on the latest threats and know the signs to look for on your network
- It's crucial to have 24/7 monitoring and analytics tools in place to watch over your network
- End users should be educated to recognize when something is wrong
- End users should be empowered to become an extension of the security team

Triage and containment

When an incident occurs, you need a cross-functional team and processes to execute a quick remediation:

- Strong security tools that protect during and after an attack are critical in this phase
- These tools should be combined with a team of professionals from across the business
- Processes should be sound and tested on a regular basis to make sure they are effective
- This team and these processes should be created before a security incident even occurs

Forensics and analysis

During remediation, you must pay close attention to how and why the breach or attack happened:

- Security tools that provide analytics and forensics are critical in this phase
- To prevent incidents of the same kind in the future, you should look for the who, what, when, where, why, and how
- Just like triage and containment, you should identify a team responsible for this function. Typically, people with an IT background or a day-to-day IT role are the best fit

Security improvement

Lastly, you must look at what was learned during the incident and use it to improve your security posture:

- As destructive as it may have been, look at each incident as an opportunity to learn
- Document areas to debrief on, including security tools, team member performance, and the effectiveness of your Incident Response Plan
- Set aggressive timelines so changes can be implemented before another security incident occurs

Building or improving upon an Incident Response Plan can feel overwhelming, especially if you lack IT bandwidth or security resources. But remember, there's never been a better time to start – and any work you do can lead to progress. Next, we'll review some of the tips we share with our customers to help them with their Incident Response Plan.

Tips for getting started

Regardless of what your Incident Response Plan looks like, these tips can help you get started or bolster what you already have in place.

1. Improve your threat detection capabilities

Tools that automate the monitoring of network traffic and user behavior can help you identify and respond to security threats faster. Often overlooked, helping your workforce understand security threats and what to look for can be a great grass-roots effort to improve how threats are detected. Remember, users are often the weakest link in an organization's security posture and a top target for cybercriminals.

2. Create a dedicated response team

This was alluded to earlier – but who should be part of this team? You should identify a leader and a team of individuals to minimize the impact of security incidents and restore operations as quickly as possible. The team should include people from IT, business continuity, communications, documentation, and even legal and HR roles.

3. Draft an Incident Response Plan

If you're just starting, don't make it complex. Start simple. All you're trying to do is document standards and ensure consistency in how you respond to security incidents. After your plan is documented, test it until you're happy with how it plays out, and the results.

4. Connect people and tools

This can be one of the most difficult parts. Connect both people and tools with the necessary capabilities from around your organization. The communications, documentation, and legal or HR roles may need access to IT systems, and everyone needs access to whatever you choose to use as a project management and communication tool. The good news is much of what you need is probably already in place. Going through this exercise can create some great conversations with everyone involved in protecting your organization and be a launching point to understanding where you have gaps.

5. Understand where you have gaps

After you go through these tips and implement some of the best practices, it's important to understand and identify where you have capability or capacity gaps. From there, you can build a plan to address them.

Additional resources

If you'd like to learn more, check out these additional resources that we have to offer around building or improving your Incident Response Plan:

- **Incident Response Checklist**

  Click here

- **Read an Expert Blog**

  Click here

- **Download an Infographic**

  Click here

How can Internetwork Engineering help?

Creating a strong Incident Response Plan

A good Incident Response Plan leads to a stronger security posture, and it should be looked at as a major component of your overall security strategy. No matter where you are in the process, we have the tools, partnerships, and expertise to help you get your Incident Response Plan where it needs to be. We can help you:

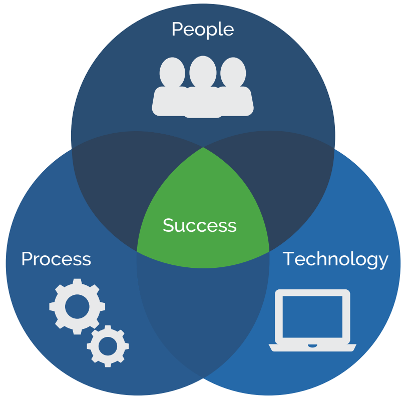
Build or improve upon your existing plan

Improve your threat detection capabilities

Improve how you respond to security threats

Accomplishing Security Everywhere, Any Way

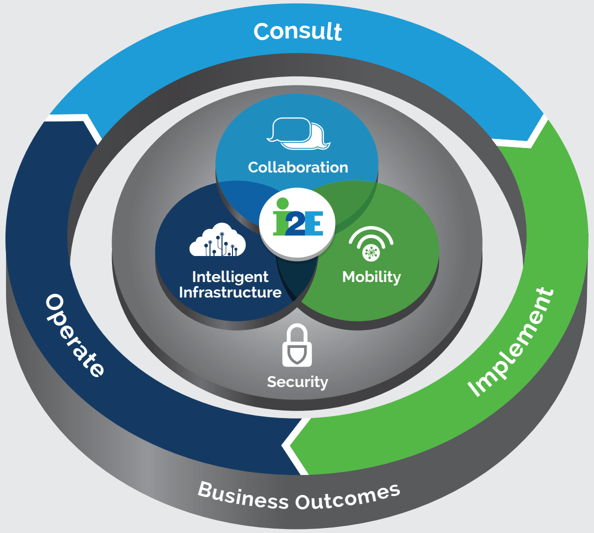
Along with helping you build and continuously evolve a strong Incident Response Plan, we can help you implement a multi-layer approach to security. We'll provide real-world perspectives that come from decades of experience across multiple industries, and leverage our process to help you detect, contain, and control security threats so you can manage risk. Based on your gaps and security requirements, we'll recommend best-in-class technology from industry leaders like Cisco and work with you to protect your endpoints, branches, campus, edge, data center, and clouds – ensuring your business, data, and reputation remain safe at all times.



Regardless of your current security capabilities, IE can enhance your security posture everywhere, any way through a combination of people, process, and technology.

Our I2E methodology

We believe that security is not a one-time event, it's a continuous process. Our I2E methodology enables us to make that a reality in your organization.



Consult	• Strategic Roadmaps • Quick Advisors • Security Risk Assessments • Security Awareness Training
Implement	• Incident Response Planning • Deployments • Installations • Updates
Operate	• Vulnerability Management as-as-Service (VMaaS) • Security Monitoring • Staff Augmentation

Need help building or strengthening your organization's Incident Response Plan?

Reach out today to schedule a meeting. We'll answer your questions, discuss your challenges, and share what we're seeing in your industry.

www.ineteng.com/contact

(704) 540-5800

About Internetwork Engineering (IE)

At IE, we are people connecting people. Since 1996, IE has been connecting people to their customers, coworkers, suppliers, patients, citizens, and students throughout the Southeast, creating more meaningful interactions with the people you care about most. Our mission is to provide technology solutions that inspire innovation and achievement, knowing that the right technology at the right time has the power to transform industries, countries, and lives.

INTERNETWORK
ENGINEERING