OSTENDIO

The 11 Step Process For Building an Incident Response Team

197 Days

is the average amount of time it takes companies to identify a security breach.

(Source: IBM)

69 Days

is the average amount of time it takes a company to contain a security breach.

(Source: IBM)

45%

of organizations worldwide will have experienced attacks on their software supply chains by 2025.

(Source: Gartner)

88%

of board members have classified cybersecurity as a business risk.

(Source: Gartner)

1. **Start with an executive or board-level support:** If you have a champion on the executive board who understands the importance of being ready to deal with security breaches, this can expedite the process of getting an IRT set up.
2. **Bring in experts to help:** Save time and money by pulling in outside experience that has the knowledge to help with your broader security program as well as your IRT.
3. **Assemble the team with reps across the organization:** Get everyone involved. Finance, PR, HR, Marketing, Legal, etc. We all have a role to play and it's important to make sure everyone knows their response during a crisis.
4. **Name a leader and define clear roles & responsibilities:** Appoint a team leader so everyone knows who is in charge when there is a serious incident. Assign and document responsibilities for each team member.
5. **Allow for logistical considerations:** Consider locations of team members, time zones and contact points for each team member. Ensure there is a way to connect in case of network connection issues.
6. **Create a register of critical assets:** Define and document what assets are critical to your company. Remember that an asset also includes people. Use a management tool to help you handle the register of critical assets so everything is always up-to-date and ready.
7. **Plan and conduct drills:** Just like you conduct fire drills, you need to test your IRP, too. Learn from the drills and improve the way the Incident Response Team handles different emergencies.
8. **Foster a culture of openness and security awareness:** People on your IRT should be encouraged to speak up if they see something significant. Build a culture of openness and security awareness that can help mitigate incidents in the first place.
9. **Invest in technology:** Serious security people invest in the right technology to get the job done. Look for a tool that will help you assign roles on the team, document steps taken to respond to an incident, and allocate responsibilities to team members.
10. **Publish and Maintain a Contingency Plan:** The plan needs to be available for the IRT to see, use and make comments/suggestions. There should be a way that comments or suggestions can be assigned within the plan to a team member.
11. **Ensure the IRT has a capability to respond to risks rated as "high":** Every company will have high-rated risks. When you identify those risks, be sure your team is equipped with the tools and knowledge to respond appropriately.

3 Reasons to Future-Proof Your Organization with an Incident Response Plan

No one has a crystal ball to see into the future—but you can always prepare, even if you don't know exactly what it looks like. An incident response plan is just one way serious security professionals future-proof their organizations and safeguard from the detrimental effects of a data breach or unfortunate event that can lead to business disruption.

Why serious security people implement people-first incident response plans:

1

Secure Your Data

Data is imporant on both a personal, and professional level. With an always-on incident response plan, you can actively protect everyone's data. Measures in place may include backups, detection alerts for malicious activity, access management, and patch management.

2

Strengthen Your Reputation

You know what a PR nightmare a security breach can be when it's not handled appropriately, and in a timely manner. A data breach leaves doubt and uncertainty in your customers' minds and damages reputation and trust. With an incident response plan, you can be ready for anything and instill confidence in your people and your ecosystem.

3

Safeguard Your Finances

Data breaches are costly, whether you're a large corporation or a small to midsize company. An incident response plan ensures you can act appropriately (and fast). The sooner you detect a security incident, the faster your team can respond and mitigate any financial risks to your organization and avoid fines.

OSTENDIO

Welcome to the next generation of security.