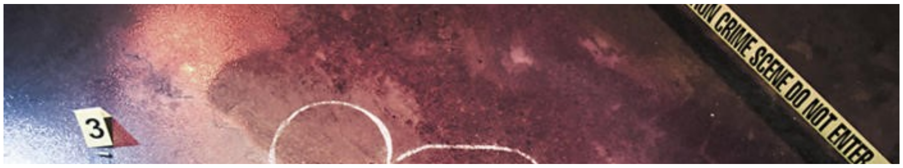
10 steps for a successful incident response plan

www.csoonline.com
6 mins read

Incident response plans are often left unused, leaving firms far less able to detect and respond to cyber attacks or data breaches. Here's our 10-point process to ensure you set up -- or improve -- an IR plan that actually works.



Thinkstock

Incident response (IR) plans are designed to test your company's ability to respond to a security incident. The ultimate goal is to handle the situation so that it limits the damage to the business while reducing recovery time and costs.

Sadly, most IR plans fail to deliver on this promise. For companies that have one -- and according to one recent survey, one in three organizations don't -- they are bare-bone, poorly set out and rarely involve any other lines of business (LOB) aside from the InfoSec and IT teams. Many remain rarely tested and reviewed, as thus not fit for their purpose when that incident strikes.

1. Address business issues and assign roles

As evidenced above, too few firms have an IR plan. For those that do, even the best laid plans can lack critical information or not include the right people.

Indeed, consultancy firm McKinsey advises that IR documentation is often "out of date" and "generic" and "not useful for guiding specific activities during a crisis." This means you need to start with the basics, implementing a plan and mapping out the right structure and laying out employee roles.

To start, McKinsey advises that early in the development process, companies should involve the people who will own and maintain the IR documentation. This will help the program transition from a special IR initiative to business-as-usual (BAU) practices. It is also important to develop other key components, like an incident taxonomy (to help with attack identification and remediation) and data-classification frameworks.

Critically, it's important that these plans truly understand the business and outline the roles certain employees will play. Some suggest having one executive to bear responsibility for implementing the plan across business units and geographies is key, too.

“The IR plan must be aligned to what’s important to the business, the company culture, how response happens to current existing issues or incidents and how response needs to change to adapt in the future,” says Sloane Menkes, principal of the cybersecurity business at PwC.

“Clearly defined roles and responsibilities are key,” added Intertek CISO Dane Warren in an interview with me last year. “Ensuring that people are trained to effectively perform those roles and responsibilities is essential.”

2. Identity relevant business departments and get them involved

As with most security problems, weak and untested IR plans often fall down because they remain the work of siloed IT and InfoSec departments. A successful, well-drilled IR plan requires inter-business collaboration, not the least because responding to a breach or security incident requires this same level of communication and business collaboration. For example, a retailer that has been breached and lost credit card information may need to involve PR (for disclosing the incident), web developers (finding and fixing software flaws), operations (to examine SLAs), marketing and customer support.

“The best way to formulate a good IR plan is to bring in the required stakeholders during the development, to ensure maximum buy-in across the organization,” says Sean Mason, director, incident response services at Cisco, who says that RACI diagrams can be useful for divvying up responsibilities .

So, who must be involved? “Outside of the typical information security teams and other supporting IT functions, a laundry list of organizations should be considered as part of an IR plan,” adds Mason. “The C-suite, critical business teams, DR/BCP, intelligence teams, human resources, legal, public relations, law enforcement, outside IR teams and vendors as appropriate.”

“Business lines have to be engaged in the planning process,” adds Neal Pollard, principal of the cybersecurity business and incident readiness practice at PwC. “For example, while IT and legal may be aligned, the business function owners may not agree with a course of action or might see other negative impacts that need to be addressed. Having insight into the business level is critical to develop a solid, well-rounded IR plan.”

3. Identify KPIs to measure the event

A good IR plan will likely be subjective -- and thus not universally clear how useful it really is -- unless there are clear key performance indicators (KPIs) as to what constitutes success. Experts believe that these KPIs can be both qualitative and quantitative. For the former, this can include the time to detection, the report an incident (important in light of the GDPR’s 72-hour report window GDPR,

GDPR → General Data Protection Regulation which goes into effect May 2018), triage and investigate. On the qualitative side, KPIs could include the number of false positives, the nature of the attack (malware vs. non-malware) and the security tool that spotted the incident.

“IR staff shouldn’t fear stats or KPIs. They are simply the measurement of management. Understand how they work and you can communicate directly to executives,” says SANS instructor Steve Armstrong. “Business uses KPIs to measure performance and response times, so choosing good ones will enable a team to pitch for more resources and better support from the organisation.”

4. Test, test and test again

Arguably one of the biggest issues here is that, while firms do carry out regular red team exercises, they don’t stress-test the IR plan enough, an exercise that should involve everyone and ideally simulate a breach. In fact, some say that firms sometimes know what this test should look like.

Running such tests keeps the IR plan updated and fit for purpose in the modern age, while also critically helping to identify (and fix) weak points in the business. This, ultimately, impacts where security budgets will be spent.

“It is important to understand that many companies are creating but not testing their IR plan,” says Pollard. “Testing can be a logistics nightmare, often requiring a full day, if not multiple days. The biggest hurdles to testing a plan are related to the timing, coordination and commitment from top executives, including the CEO. Testing also requires executives to discuss issues that don’t necessarily impact each specifically on a daily basis and therefore may be regarded as less time-sensitive.”

5. Review the plan constantly

IR plans must be revised frequently and especially as the company grows. “An IR plan should be robust enough to provide a great framework to operate within, but flexible to handle nearly every situation thrown at it. Flexibility relates to how easily it can be updated- and it should be reviewed and possibly updated quite regularly,” says Mason.

6.Determine what an incident is

Linked very closely to KPIs is the definition of what - and what isn't - an incident. By doing this, you figure out what should be acted upon and what should be ignored, while also ensuring your security team are only working on the most serious issues.

For example, is an attempted attack an incident, or does the attacker need to be successful to warrant response? Once defined, firms should conduct an incident threat analysis by discovering and documenting the threats, risks and potential failures impacting their organization’s current security measures.

One useful guide is the incident topology from the National Institute of Standards and Technology (NIST), which defines incident categories broadly as unauthorized access, malicious code, denial of service and inappropriate usage.

8. Form your team, led by a seasoned IR analyst

Incident response teams analyze reports of security breaches and threat intelligence in order to develop the organization’s incident response strategy. There are various types of incident response teams that can be composed internally, externally or a mixture of both.

Some suggest that while this process must involve various stakeholders, inside and out of IT (including lead investigator and IT director), it’s still the case that it relies heavily on experienced penetration testers and IR leads. “Usually, teams include a range of skills across the individuals the most important ones being host and network forensics,” says Armstrong. “Additionally, good teams regularly include memory analysis experts, malware analysis and threat intelligence skills.

“However, don’t overlook pentest and good hunt team skills so both offense and log analysis skills have a part to play too. For an IR team manager, a seasoned IR analyst who can do all this and understands how executives speak and think - that’s the unicorn you seek (they do exist!),” he adds.

9. Implement the right tools

“A good IR plan will center around visibility and understanding of the network, detection of the attacker, suitable alerting, secure communication for the team, and good liaison with the rest of the business,” says Armstrong. “Good threat intelligence will assist the visibility and understanding of the attackers’ activity and good communication will allow the IR team to explain the breach to the rest of the business so they can plan the remediation.”

10. Establish a communications strategy

Communication is essential at all times for incident response, and it’s particularly important you have a communication strategy for how you are to alert third parties and, if appropriate, internal teams. Externally, law enforcement and potentially breach remediation providers should be notified, while employees should be the top of the list for internal communication. They should be aware of the incident response plan (if possible), have access to it and most critically receive training on the process, so to best understand their role.