beazley

Beazley Breach Insights

Incident Response Plan – Why You Need One and How to Create It

The old adage "If you fail to plan, you are planning to fail" rings true across many areas; information security and data breach response are no exceptions. Information is a valuable asset of every business, and when the security of that information is breached, organizations face a minefield of potential liability and reputational damage.

After helping our insureds respond to more than 4,500 data breaches, Beazley's Breach Response Services team knows that organizations with a well designed incident response plan typically negotiate this minefield far better than organizations without a plan in place. A haphazard response often makes the consequences of a data breach much worse.

What is an incident response plan?

An incident response plan (IRP) is a written roadmap by which organizations intake, evaluate, and respond to a *suspected or actual breach* of computer systems or the *theft, loss, or unauthorized disclosure* of personal information. An IRP is distinct from a business continuity or disaster recovery plan. Unlike those documents, the primary purpose of an IRP is to manage privacy or security incidents in a way that limits damage, increases the confidence of external stakeholders, satisfies legal obligations, and reduces costs.

The most effective IRPs also are drafted to be triggered by suspected breaches of data across the organization and its systems, regardless of the data's department or location; human resources data, employee health plan data and data maintained by vendors should all be covered by the IRP. The IRP should also cover the organization's data on mobile and personal devices, data on any medical devices, and data stored in copiers, fax machines, or scanners.

We believe the main reason to develop an IRP is the tremendous value it provides when responding to an actual information security incident; but having an IRP isn't just sound risk management, it's also required by a number of laws, regulations, and industry standards. Whether your organization takes payment cards,[1] is a Health Insurance Portability and Accountability Act (HIPAA) covered entity,[2] is a regulated financial services firm,[3] or simply operates in certain states,[4] some type of IRP is a necessity.

The incident response team

Typically, organizations start the IRP drafting process by first appointing an incident response team (IRT) – i.e., the individuals who will actually perform the substantive tasks at hand. Recognizing that no two organizations are alike, we recommend designating a primary and secondary representative from at least each of the following stakeholders:

- Legal
- Information security/information technology
- Risk management
- Communications
- Human resources
- Privacy office (applicable to healthcare)
- Physical security
- Business continuity

Other individuals outside the core IRT may certainly be called upon as necessary; however, the departments outlined above tend to have the heaviest involvement in incident response scenarios. A good incident response plan not only identifies the key stakeholders but also establishes processes around when one department engages with another. The IRP should outline the IRT's respective roles and responsibilities, provide contact information for them across several channels (email, direct dial, mobile, and off-band in the event corporate communications are down), and speak to when the standing members of the IRT draw in additional internal and external members to assist.

Not defining the team: what can go wrong?

IT discovers a red flag and decides to investigate internally before notifying anyone else. The investigation takes 32 days and reveals that sensitive personal information was compromised. IT then notifies the legal department about the situation, only to learn from legal that the state law deadline to notify affected individuals was 30 days from the moment of discovery. The deadline has been passed, and regulators will be asking why.

Classifying the threat level

The next key area to focus on is incident classification. When it comes to information security incidents, no two are entirely alike, and each will require different response mechanisms and IRT member participation. A good IRP foresees this and triages incident types based on an easy-to-use set of criteria. Here, for example, are three simple threat levels:

- **Level 1.** It can be determined that no mission-critical systems or resources are at risk and no confidential information or personally identifiable information (PII) has been accessed.
- **Level 2.** Mission-critical systems or resources may be at risk, or confidential information or PII may have been accessed.
- **Level 3.** Mission-critical systems or resources are at risk, or it has been determined that confidential information or PII was, in fact, accessed by an unauthorized individual.

The threat levels are not intended to be overly rigid. It's impossible to capture every type of potential incident, and taking too long to determine where a specific incident falls only wastes much needed time. Further, incident response is fluid: an incident may start at level 1 and, after some analysis, be upgraded to a level 2. The main benefit of defined threat levels is the guidance they provide for next steps in each phase of the response.

For instance, a good IRP using the criteria above would note that upon discovery of a level 2 incident the first responders would immediately call together the IRT, notify their insurance carrier, and begin to prepare the network and affected systems for forensic analysis.

Preserving evidence for investigation

Preserving evidence for forensic analysis can be crucial in incident response, and a good IRP recognizes that in certain situations the desire to restore operations must take a back seat to preserving the environment for forensic analysis.

Although the precise technical steps an organization's first responders need to take when investigating a suspected network breach is outside the scope of this paper, we encourage you to access and review our *Information Security First Responder Guide*,[5] which includes the best practices of technical incident response.

Not keeping the forensic investigation in mind: what can go wrong?

IT/IS identifies a server that has been infected with malware. The malware appears to be capable of exfiltrating data, and the team works quickly to eradicate the malware and rebuild the affected server from a recent back up. A few days later, an external forensic firm is engaged to help determine what happened. Unfortunately, the IT team did not take a forensic image of the server prior to rebuilding. Additionally, important logs that would have given further visibility into the attack are no longer available as the company only keeps them for 48 hours. Evidence that might have shown only a small number of records had been affected or that no data had been exfiltrated at all is now gone for good.

Communicating about the incident

A well thought IRP does not, however, just stop at the technical component of the investigation.[6] It continues to provide a roadmap for how to move forward once the technical investigation has confirmed the theft, loss, or unauthorized access to personally identifiable information. To that end, a well designed IRP speaks to the actual methodology behind responding to a confirmed "data breach," as that term is defined under the state or federal laws that apply to the organization and the type of data.

The IRP is not intended to take the place of actual legal analysis or public relations guidance, but it should outline what the organization needs to accomplish once it appears that a data breach may require notification to affected individuals, regulators, or the media. Without set guidance in the IRP, organizations struggle on what to say, how to say it, and when to say it. Quite often, even well-meaning intentions not filtered through the IRP result in unnecessary damage to the organization.

Premature communications and notifications: what can go wrong?

Your company uncovers malware on the point of sale devices in one of your stores. Before the IRT has a chance to finish analyzing the malware's capabilities or reviewing the operative data breach notification laws, your CEO decides that the company must issue a press release the following day, stating that 200,000 customers' cards may have been impacted. The press release links to the company's website, with a video message from the CEO apologizing about the "breach." After contacting your insurance carrier and engaging with an outside forensic expert, you determine that the malware on your point of sale environment failed to actually steal any card data, and that this matter was a non-event, and required no public notification. In the meantime, the share price has taken a hit and many customers will take months to return.[7]

Avoiding common pitfalls when drafting an IRP

If you're in the early stages of assembling an IRP for your organization, there's no need to reinvent the wheel. Beazley Breach Response policyholders are able to draw from a variety of battle-tested IRP templates on our proprietary risk management portal, BeazleyBreachSolutions.com. We strongly encourage you to make use of the content there as a starting point for your IRP. But whether you're just starting or have a plan developed already, we recommend steering clear of the following issues we see present problems for organizations over and over again.

The “B” word

The IRP is an “incident” response plan, not a “data breach” plan. “Data breach” is a legal term with a specific meaning. A good IRP avoids using that term entirely. Members of the IRT should not refer to an incident as a “breach” in writing or during the investigation. Leaving an email or paper trail of “breach” references could be particularly problematic if the investigation concludes notification is not required because there is no breach under relevant law. Don’t provide ammunition for regulators or plaintiffs’ attorneys.

“Must” or “shall”

The IRP should avoid language suggesting that steps in the process are mandatory. Each incident is different, and you may need to follow different steps depending on the situation. Allow flexibility and don’t put yourself in a position where a regulator or attorney can question why a certain step wasn’t followed.

Too long

The IRP should be easy to use in a crisis. If it’s too long or detailed, members of the IRT are less likely to stay familiar with it.

Too short

On the other hand, the IRP needs to have enough information to be useful, so everyone on the team understands their role and it’s clear how to call upon resources outside the organization when necessary.

“It’s just paper”

While organizations often focus on electronic incidents, paper records are protected by a number of state laws, as well as federal statutes like HIPAA for health information and Family Educational Rights and Privacy Act (FERPA) for student records. The IRP should cover data regardless of the format in which it’s stored, so you can react just as quickly.

“Gone fishin”

Incidents are guaranteed to be discovered at the least convenient time – on a Friday afternoon or weekend, or when an essential person is travelling. Be sure to include the ways to reach team members 24 hours a day and have backups for members in case they’re unavailable.

Conclusion

The reality of information security today is that the idea of an “impregnable” network perimeter, able to keep intruders at bay, is long gone. Whether it comes about because of a determined and skilled hacker or simple human error, a data breach is no longer an “if” but a “when.” To assume otherwise, and not prepare for the minefield, will greatly harm your organization’s brand, balance sheet, and business. But with a well thought-out IRP that follows the principles outlined above, a plan that you test and update regularly, your organization will be better equipped to turn a potential crisis into a manageable bump in the road.

We strongly encourage you to take the time to review BeazleyBreachSolutions.com for more cutting-edge content on all things information security, privacy, and incident response planning.

[1] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures § 12.10 (ver. 3.2 April 2016), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf.

[2] 45 C.F.R. § 164.308(a)(6), discussed in U.S Dep’t of Health & Hum. Svcs., HIPAA Security Series no. 2, Security Standards: Administrative Safeguards, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.

[3] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice I.A.2(c), 70 Fed. Reg. 15,736 (Mar. 29, 2005), https://www.gpo.gov/fdsys/pkg/FR-2005-03-29/pdf/05-5980.pdf.

[4] See, e.g., Standards for Protection of Personal Information of Residents of the Commonwealth, 201 Code Mass. Regs.§ 17.

[5] Available to Beazley Breach Response policyholders at BeazleyBreachSolutions.com.

[6] Indeed, for information held in certain formats (e.g., paper) or involving simple and inadvertent disclosures, the technical members of the IRT may be entirely unnecessary.

[7] According to KPMG, 19% of retail shoppers would not return after a hack compromising personal information, and almost 50% of the remainder would take three to six months to return. KPMG, Consumer Loss Barometer (July 2016), available at https://info.kpmg.us/consumer-loss-barometer.html.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.