Deloitte.

Deloitte Discovery

Discovery insights
5 questions on data breaches and incident response

An interview with Michael Weil, Deloitte Advisory Director in the Discovery practice of Deloitte Financial Advisory Services LLP.

In today's digital world, the response to a data breach is both critical and complex. The response is critical because sensitive information, such as intellectual property, product specification and manufacturing techniques, or Personally Identifiable Information (PII), may be exposed or released. Likewise, the response is complex because it can affect the specific needs of multiple stakeholders in your organization. These stakeholders, such as business operations, IT, the Office of General Counsel and Human Resources can all have a stake in the incident response. Thus, a proper incident response program should implement a multi-faceted approach with unified coordination.

Questions	Michael Weil's take
Incident response is not a new concept in network security, so why is it becoming a focus for corporations now?	Any organization with information worth stealing is a target — no one is immune. It is not an "if" you are hacked, it's a "when" you are hacked. As many organizations have moved to the network enterprise in an effort to improve efficiency, the network threat environment has become more volatile and organizations may be at a heightened risk of compromise. With the increasing threats posed to intellectual property and data, many organizations are proactively deploying strategies to combat attacks and protect their data. They are often focused on protecting data in a way that combines network security measures and incident response programs. As the threats from unknown groups, individuals, and foreign countries continue to grow, organizations should continue to strengthen their incident response programs. Adversaries can now effectively take millions to billions of dollars' worth of data and affect the viability of companies. Boards of Directors and senior executives have taken notice that computer incidents have the potential to impact their balance sheet, bottom line, and shareholder value. Rather than spending years entering a market by legitimately developing products and services to compete with a corporation, the adversaries can abscond with a company's materials through computers for a significantly lower cost.

Questions	Michael Weil's take
How can policies regarding non-business use of computers on the company's network impact the overall security strategy?	What I sometimes find surprising is that with all the security and data protection measures organizations employ to protect themselves from external threats, they often downplay or neglect the internal threats. For example, a company may have firewalls, intrusion prevention and detection systems, and other network sensors and monitors, but even with the best information security policies and practices in place, a glaring threat to the corporate network is often personal use of the corporate network by employees. These outside threats can arise when employees visit unsafe websites, or check personal email and may inadvertently execute malicious code sent to them in attachments or embedded websites. When developing network security policies, companies should look at a host of issues that could pose a threat if they were infiltrated. Network security should take into account the personal use practices of their employees, and look at solutions that can protect their network from attacks. An organization can have the best security perimeter protecting its network, but the weakest link to the perimeter could be an individual on the inside. In addition to the insider threat, security policy and practice should consider personal use as it relates to phishing attempts, social engineering, malicious websites, and other threats. With many organizations becoming more globally connected and expanding internationally, renewed focus on the insider threat and personal use policy can assist with data protection.
What departments are typically involved in an incident response and how do they work together?	Incidents often bring together many of a company's functions to aid in repelling or recovering from an incident. From the matters I have worked on, they can include: • The affected business unit • In-house counsel • Outside counsel • Insurance companies • Information Technology • Human Resources • Public Relations • Customer Relations • Investor Relations • Board of Directors • Risk Management
What should I do if I suspect a compromise?	You should have an incident response plan in place that activates at higher levels as the severity of an incident increases. Despite the best plans and defenses, system compromises can happen. Your information security team can help identify the potential severity of the attack and execute your incident response plan. If you do not have an information security team or qualified individuals, you can contact an organization specializing in computer incident response. Once you understand the nature and severity of the attack, you may need to make prompt decisions about: • Taking impacted systems offline • Resetting credentials • Deactivating accounts • Working with business units to determine the operational impact of remediating the compromised systems • Investigating the compromise • Determining the business damage from the compromise • Recovering from the incident Some of the response steps can yield prompt, actionable results, but many of the steps can take time to yield useful or helpful information. Remember, the incident is not a crime drama television show where the crime is resolved in an hour. It may take a few weeks to have a more informed understanding of the intrusion method and data compromised. In the meantime, the incident responders should make recommendations that mitigate further damage and reduce further system compromise.

Questions	Michael Weil's take
How should incidents be handled?	A team of specialists in networks, computer forensics, incident response and crisis management should be assembled with a focus on key areas such as: compromise method, damage assessment and compromise attribution. The compromise method identification should examine the existing system logs, memory, and data for suspicious activity and the points of entry into the systems. Compromise investigations should also seek to identify additional system locations where the attacker may have ventured, the level of access the attacker obtained and the methods used in the attack. In the damage assessment, a team of specialists help to determine if data exfiltrated the network and if any outbound data can be recovered. Often times, outbound data is encrypted and additional tests are performed to identify the files opened by the attacker, which can provide an approximation of the areas where the attacker was primarily interested. The damage assessment should also consider the type and age of data compromised to aid in strategic business decisions in the case s of intellectual property theft and governmental reporting requirements when PII or health information is the subject of the compromise. The damage assessment portion of the investigation should work closely with the business unit to understand the nature of the data compromised to assist in understanding the extent of the attack and the data the adversary seeks. Attribution of a compromise, or determining the attacker, can be extremely difficult and may never happen because attackers often take steps to protect their identities. However, the incident response team can look for trends or patterns in the attack to narrow down the field of potential attackers.

My take: Collaboration and coordination are key factors in incident response programs

As organizations prepare for threats by strengthening their network security measures, they should simultaneously seek to improve their incident response programs. Working with a team of specialists can help to improve an organization's overall network security strategy by coordinating the needs of the various business units involved.

Contact

For more information, please contact:

Michael Weil
Director, Deloitte Advisory
Deloitte Discovery
Deloitte Financial Advisory Services LLP
miweil@deloitte.com
+1 312 486 0207