KPMG

10 Common cyber incident response mistakes

Cyber insights for the federal government

Today's reality:

– A proactive and comprehensive incident response program is a critical element of information security.

– When the integrity of a computer network or information system is compromised, responding appropriately will minimize business disruptions and reduce the impact on the agency's mission.

– Ten major mistakes can hinder an agency's response effort to data breaches, cyber attacks and other serious security events.

Does your incident response program solve or exacerbate your security problems?

In the unpredictable and fast-paced battle against cyber attackers, well-prepared incident response teams are a powerful weapon in an agency's arsenal. Responsible for assessing security systems and responding to security threats, incident response teams play a major role in resolving issues and controlling damage of system breaches, malware exposure, and other security events.

Addressing ten common incident response mistakes can help organizations determine if their incident response teams are capable of solving, rather than exacerbating, their security problems.

Mistake #1: Plans are not tailored to the agency.

Many organizations implement boilerplate incident response plans that enumerate, in extensive detail, every step that should be taken to investigate a potential incident. While this may feel thorough and reassuring, it can often overcomplicate response procedures and slow down or work against investigations. Off-the-shelf plans are often outdated and ineffective against evolving threats and changing technology.

Advice from KPMG LLP (KPMG): Organizations should establish policies, processes, and procedures that are tailored to their culture, environment, response personnel, and most importantly, business objectives. Documentation should be concise, and should evolve constantly to remain current with both federal trends as well as shifts in business objectives.

Mistake #2: Plans are only used in real-world incidents.

In information security, planning only goes so far. Organizations create comprehensive incident response plans but sometimes do not test them until a real event occurs, only to find they fail at the first step. Additionally, many organizations view creating an incident response plan as a one-time event as opposed to an ongoing process. As a result, plans have incorrect information regarding tools and people, or detailed steps that do not work or are out of order.

Advice from KPMG: Agencies need to put their plans into action with regular frequency before a real incident occurs—similar to the way fire drills are performed. Lack of exercising an incident response plan could result in increased response time, confusion, and worst, an exploit.

Mistake #3: Teams are unable to communicate with the right people in the right way.

Because many IT security organizations are characterized by segmented functions such as vulnerability scanning, patching, and system administration, it can be a major challenge to find, coordinate and communicate with the key parties involved in responding to an incident.

Advice from KPMG: A centralized communication dashboard, where the incident response team can post details about the current investigation and pull the information as-needed, can help limit the disruptions of constant e-mail messaging, which can overwhelm e-mail inboxes and lead to missed messages or conflicting information. Additionally, this dashboard system can be configured to limit access or add people as needed, without sending duplicative e-mails.

Mistake #4: Teams lack skills, are wrong-sized, or mismanaged.

All agencies, regardless of size, face challenges when it comes to choosing the right personnel to staff the incident response team. With limited security budgets, small agencies may assign incident response duties to system and network administrators, who possess technical knowledge and historical understanding of how systems operate, but no experience making business-impacting decisions amid a crisis or breach. On the other hand, large agencies struggle to allocate the most efficient number of resources to the incident response team, assuming more personnel equals greater capability. This can lead to overlapping efforts.

Advice from KPMG: Organizations should closely evaluate the need for additional training or internal recruiting assistance to help foster the proper level of experience on the incident response team. In addition, strong leaders who oversee the team should clearly define roles and responsibilities, promote greater collaboration, and improve communication to, and beyond, the team.

Mistake #5: Help desk activities can destroy critical evidence.

From strange computer behavior to frequent account lockouts to multiple antivirus alerts, computer issues that may signal a malicious code infection are often first reported to the help desk. If help desk staff members are not well versed in the needs of incident responders, their work to fix user issues may destroy key evidence. For example, installing software, running antivirus or cleaning tools, or adjusting system settings can overwrite information that may be invaluable to incident responders. Piecing together the chain of events can be impossible, especially if the initial actions were not documented. Agencies who use subcontractors as their IT Helpdesk should make sure their helpdesk staff are aware of the indicators that need the involvement of the incident response team.

Advice from KPMG: If they suspect a user issue may be caused by malicious code, help desk staff should capture a memory image of the system prior to making any other changes. The help desk should also be trained to document their activities in case their actions become part of an investigation.

Mistake #6: Incident response tools are inadequate, unmanaged, untested or underutilized.

Organizations may see their incident investigation and remediation processes experience unexpected delays, or even grind to a halt, if the tools teams rely on to unearth information about affected systems and people are mismanaged or misused. Even the latest and greatest technology solution can fail to provide a consistent, reliable output without proper planning, investment, and maintenance.

Advice from KPMG: Agencies should maintain an inventory of tools in a centralized location and establish processes to help ensure timely license renewal and functional component upgrades. In addition, team members should be trained across the entire tool set on an ongoing basis. Finally, tools should be regularly assessed to determine if they can address the most current threats.

Mistake #7: Data pertinent to an incident is not readily available.

When information containing the relevant details of an attack does not exist or is not readily available, there is a cascading effect throughout the incident response process. Ultimately, the incident response team struggles to assess the impact, contain the damage, and communicate to management.

Advice from KPMG: Addressing this issue requires organizations to understand what data sources they have, what data they are capable of producing, and how they manage their data. Engaging technology owners and evaluating the asset management system are both good ways to uncover the full range of potential data sources. In addition, the incident response team should identify signaling events (e.g., failed authentication, logs purged, interactive log-on, etc.) that could provide contextual information about an incident, and establish processes for aggregating, storing, and making sense of this data.

Mistake #8: There is no "intelligence" in the threat intelligence provided to incident responders.
Threat intelligence (TI) is a buzz-worthy topic in IT security; and threat intelligence products are flying off the shelves, but many organizations find that purchasing all available threat feeds does not result in complete threat detection. Often, incident responders are overwhelmed with hashes, file names, IP addresses and other indicators, but given little or no context as to how these indicators may affect their organization.

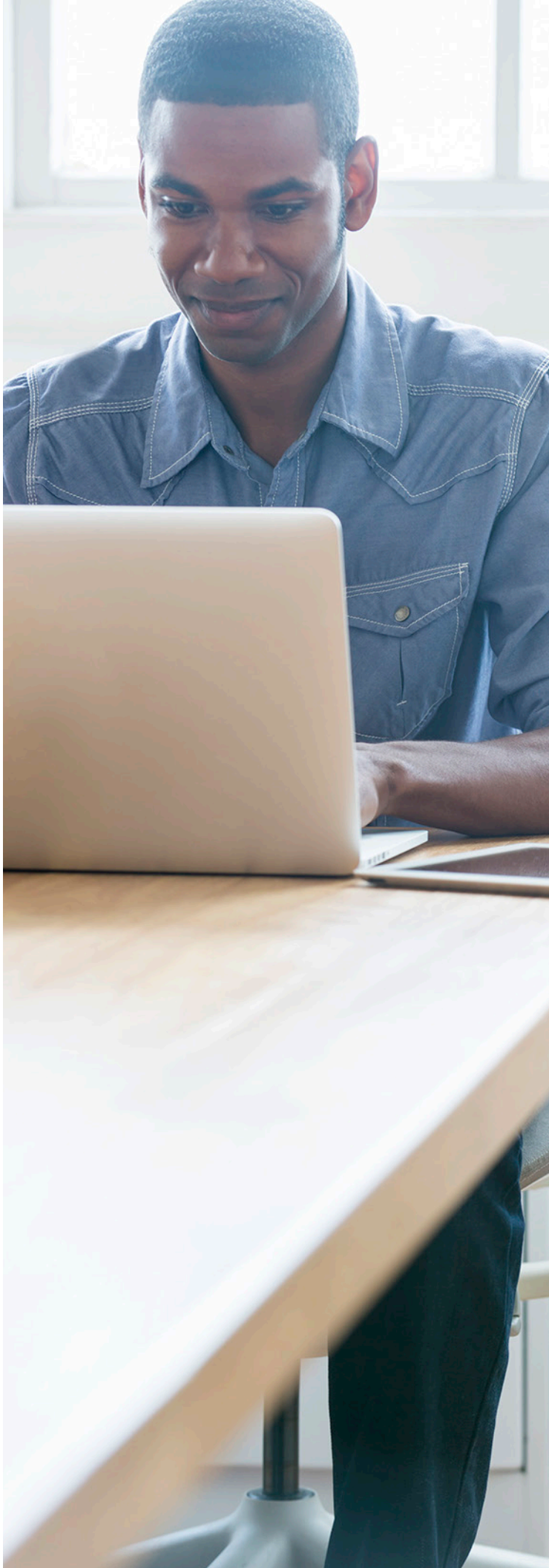
Advice from KPMG: Organizations must integrate threat intelligence into incident response and actively work with their TI vendor help to assess if the intelligence is actionable and valuable for their agency.

Mistake #9: The incident response team lacks authority and visibility in the organization.
Political disputes can work against the incident response team's efforts, waylay the response process, and prevent timely incident resolution. It is rare that incident response teams operate with the ultimate authority to make the business changes to secure the organization. Rather, they must escalate issues to management to receive the necessary traction, sometimes as incidents worsen.

Advice from KPMG: Management must fully support the incident response team, its mission, and its activities during an investigation. Incident response should be communicated and marketed as a service that maintains the integrity of the organization, not as the group that creates more work. Additionally, the incident response team should engage other teams to nominate a primary contact to facilitate participation in the incident response process.

Mistake #10: Users are unaware of their role in the security posture of the organization.
Exploiting users is one of the most common, and easiest, ways that criminals compromise organizations. Finding a vulnerability that gives an attacker full access to a network can be a lot of work, but crafting an e-mail message that convinces a user to run malware is child's play. Unfortunately, educating users about threats only goes so far.

Advice from KPMG: Agencies' security management team should continuously educate users not only about common exploitation practices, but also about information security's role within the organization. By doing so, users can be active participants in security. They will know where to turn and trust the process, rather than attempt to solve security problems on their own by installing untrusted tools and potentially causing greater problems across the network.



About KPMG Forensic[SM]

KPMG comprises a global network of professionals. Many of these professionals are leaders in the Cyber Security community, helping develop the tools and methodologies used to combat cyber crime on a daily basis. Our professionals have experience working on all forms of cyber crime including insider threats, data breaches, hacktivist groups, and Advanced Persistent Threat-style intrusions by highly motivated adversaries.

KPMG is also heavily involved in the information security community. This involvement provides us with early insight into emerging issues, which we share with our clients and the project support teams as a component of our advisory role. The pragmatic advice and the services we can offer are shaped from the experience we have gained and relationships we have developed serving clients of various size, scope, and complexity.

KPMG is a preferred provider of Incident Response services to many organizations and acts as an extension of other organizations' internal teams. Since KPMG is independent (e.g., tool agnostic) and vendor neutral, clients can gain comfort in knowing that KPMG is entirely driven by our experience with similar organizations (references available) and our confidence in our ability to provide value-added assistance.

Contact us

Edward L. Goings
Principal, Forensic Technology
Practice Co-Leader
T: 312-665-2551
E: egoings@kpmg.com

Ronald E. Plesco
National Lead, Cyber Investigations,
Intelligence & Analytics Technology
T: 717-260-4602
E: rplesco@kpmg.com

David B. Nides
Director, Forensic Technology
T: 312-665-3760
E: dnides@kpmg.com

Dominique M. Kilman
Manager, Forensic Technology
T: 210-270-1659
E: dkilman@kpmg.com

Tony Hubbard
Principal, Federal Advisory
T: 703-286-8320
E: thubbard@kpmg.com

David Buckley
Managing Director, Federal Advisory
T: 703-286-8489
E: davidbuckley@kpmg.com

Ken Adams
Director, Federal Advisory
T: 703-286-8102
E: kennethadams@kpmg.com

kpmg.com/us/forensic

kpmg.com/socialmedia

This document is a revision of *ForensicFocus: 10 common cyber incident response mistakes.* Authored by Edward Goings, Ronald Plesco, David Nides, and Dominique Kilman of KPMG LLP.