DARKReading

WEBINAR SUMMARY

July 22, 2021

Building an Incident Readiness and Response Playbook

Ryan Clancy, Compliance and Assessment Division, Motorola Solutions
Jake Williams, President & Founder, Rendition InfoSec

KEY TAKEAWAYS

- IR playbooks need to go broad, not deep, at least initially.
- The IR plan guides whether threat containment or eradication is the default approach.
- Cyber insurance requirements can impact law enforcement involvement.
- Poor planning for evidence preservation increases response time and difficulty.
- Regulatory compliance requirements can impact crisis communication.
- IR planning is a key part of threat prevention.

in partnership with

MOTOROLA SOLUTIONS

OVERVIEW

Today, it's not a matter of "if" a cyberattack happens, but "when" it happens. When it does happen, emotions and stress levels are usually very high as companies respond in crisis mode. Creating an incident response (IR) plan now, before an attack occurs, provides organizations with a map of what they need to do in their response.

IR planning goes beyond the IT or security operations teams; it includes people from across the company who are responsible for components of the plan, such as public relations, legal and regulatory compliance, and procurement. The plan covers everything from how to make sure that logs and other critical evidence are captured to when and how to include law enforcement.

CONTEXT

Jake Williams and Ryan Clancy discussed the importance of IR plans and what organizations need to consider as they develop these critical playbooks.

KEY TAKEAWAYS

IR playbooks need to go broad, not deep, at least initially.

When creating an IR plan, the focus needs to be broad, providing guidance on how the organization expects to execute in the incident response space when an attack occurs. The exception is if an organization has identified very specific problem areas that pose a big risk to the business; in those rare situations, a company may choose to go deep on a specific, very real problem first.

> Go broad and get something down on paper. . . . The threat actor is not waiting for you to get your incident response plan done.
>
> *Jake Williams, Rendition InfoSec*

One of the very first steps in developing a broad IR plan is to identify and document the IR team members and their roles and responsibilities, including a few sentences about what each individual unit is expected to do during an attack.

Common IR team members

- IR staff
- Internal legal counsel
- Procurement
- External legal counsel
- Business unit leaders
- Public relations
- Physical security
- Compliance
- Union representatives, if applicable
- IT and systems engineering

The IR plan guides whether threat containment or eradication is the default approach.

Although every incident is different, starting with a default strategy—containment or eradication—saves significant time when responding in a crisis. If a situation requires it, the team may consciously decide to veer from the default strategy.

Contain or Eradicate? The benefits of the two approaches

Containment Benefits	Eradication Benefits
– Threat actors rarely have a single backdoor in a network. – Additional cyber threat intelligence (CTI) is gained by studying threat actor actions within the network. – When balanced with protecting critical data and assets, usually results in a more measured incident response.	– Gets the threat actor out of the network, at least as far as the company knows. – Not as likely to invoke hindsight bias; e.g., "We could have prevented any data exfiltration!" – Easier to defend to regulators. – Promotes bias to action.

If the organization cannot agree on a single default approach, including described scenarios and approaches in the IR plan can close that gap.

Cyber insurance requirements can impact law enforcement involvement.

Deciding whether to involve law enforcement and when to include them is a tricky question for many organizations. The first consideration is insurance: if an organization has insurance that covers cyberattacks, they need to first ask the insurer what law enforcement reports (e.g., local sheriff's office, Federal Bureau of Investigations, the Internet Crime Compliance Center), if any, are required to process the claim.

The notification options an organization can choose to take fall into one of three broad categories.

- **Notify at outset.** Law enforcement is made aware of the incident *when it occurs*.
- **Notify at conclusion.** Law enforcement is made aware of the situation *after the incident investigation is complete*.
- **No notification.** The business does not make law enforcement aware of the incident.

Even when law enforcement is notified, the organization is still responsible for performing its own incident response and remediation. Law enforcement can add additional context around the indicators of compromise.

Poor planning for evidence preservation increases response time and difficulty.

The IR plan needs to include evidence preservation priorities for any data not regularly forwarded to a security information and event management (SIEM) solution. Without a plan in place, critical logs and information that can help the organization quickly and efficiently respond to a problem are likely to be missing.

> You have to have an evidence preservation plan. Logs will not save you if you don't have a plan to preserve them.
>
> *Jake Williams, Rendition InfoSec*

As part of the plan, organizations need to collect the most volatile data not being stored elsewhere first. All critical systems need to be considered, even if they are not yet in scope, because they may need to be included in the plan.

Key considerations in planning for evidence preservation

Remote sites	Have a plan for obtaining evidence from remote sites, particularly those without dedicated IT staff. This may include shipping or having an IT team member courier drives from the remote site if the IR software is likely to take longer to collect data from the remote office.
Windows considerations	– Increase event log sizes on every Windows machine (workstations and servers) beyond the default Security event log size of 20 megabytes (MB). – Know what is and is not being logged. – Enable non-default logs, such as: - Process auditing (with command line - Share access auditing (basic, not advanced) - Failed logins - Sysmon (be careful with Sysmon filters)
Linux considerations	– Examine logrotate configurations and increase log retention if there is adequate disk space but be aware of additional billing in cloud deployment models. – Consider enabling iptables logging and auditd. Note that some endpoint detection and response (EDR) products use the auditd socket, so enabling it provides some logs but also breaks the EDr. – Use an expert with experience in configuring the auditd to log the right amount of data.

Regulatory compliance requirements can impact crisis communication.

Organizations need to plan for how they will communicate with vendors, stakeholders, customers, and other audiences during and after an incident. Regulatory compliance requirements can play a role in this planning, and knowing who, when, and how to notify needs to be understood before a crisis occurs.

Communicating an incident is not a one-size-fits-all endeavor; each communication needs to be crafted for its target audience using a consistent message. Investigations that are not yet complete should include a timeline for when additional details will be communicated, and organizations need to stick to a stated timeline.

Additionally, procurement and vendor/supplier relations need to be part of the IR team to help define the contractual requirements that impact notifications. Some contracts have their own definition of what constitutes a reportable incident.

Regulations can also stipulate where data can—and cannot—be sent and handled. This can impact the ability to ship data, especially outside of the country, as well as how an analyst brought in to help with the investigation handles that data.

IR planning is a key part of threat prevention.

Preparation for an incident through IR planning, training, playbook development, and tabletop exercises is a critical component of threat prevention. Vendors like Motorola Solutions can help organizations tabletop exercise and assess the readiness of the organization against security compliance standards, identifying and filling gaps to create a quality IR plan.

Ten considerations for designing an incident response plan

Reduce boilerplate information	Remove anything that prevents the IR team from finding what they need quickly. Include a title page, documentation control information, and a table of contents, and then jump into actionable information.
Place important information at the front	Put the actionable information up front and use action words. Don't make responders search for information.
Use visual elements	Use tables rather than blocks of text as much as possible. For example, use a table when discussing priority levels, roles and responsibilities, and notification plans.
Create clear roles and responsibilities	Define team members and departments, and what they are expected to do in a crisis.
Focus on internal and external communications	In addition to communicating externally, notify employees and contractors and share a phrase or talking points so they can stay on message.
Include cyber insurance information	Document the requirements for cyber insurance and the notification requirements.
Include vendors in planning	Related vendors, such as outsourced IT teams and critical service vendors, need to be included in response planning and testing.
Don't go overboard with playbooks	Playbooks are living documents; too many or too long decreases the likelihood they will be maintained.
Practice the plan	Use tabletop exercises of real-world scenarios to practice the plan. Using an outside company with IR plan experience, like Motorola, can help identify gaps.
Focus on compliance requirements	Document what each compliance body requires when an incident occurs, including notifications. These requirements vary among regulatory bodies.

> Prevention and preparation is key. This is where I would focus a lot of time and attention.
>
> *Ryan Clancy, Motorola Solutions*

OTHER IMPORTANT POINTS

- **Budget for IR up front.** Budgeting for unknown incidents and responses is challenging, but it needs to be done up front. If IR is not budgeted for, when an incident occurs, critical time is spent finding the money in the organization, meaning the response time lengthens, as does the overall cost.
- **Motorola Solutions can help with IR planning.** For more information, reach out to Ryan Clancy: ryan.clancy@motorolasolutions.com; 719-651-3632.

BIOGRAPHIES

Jake Williams

Founder and President, Rendition InfoSec

Jake Williams is a computer science and information security expert, U.S. Army veteran, certified SANS instructor, and course author. Jake has over a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering space. He is a former network exploitation operator with the DoD where he is one of fewer than 15 people to date who have earned the designation of Master CNE Operator.

Ryan Clancy

Managing Consultant, Motorola Solutions Inc.

Ryan started his career in the military as a cyber warfare officer for the US Air Force. From there he joined the commercial space focusing on cyber intelligence and incident response. Ryan has taken on customers in a variety of sectors including energy, finance, healthcare, and defense. Currently, Ryan leads the compliance and assessment division for Motorola Solutions Inc.