Secureworks®

WHITE PAPER

5 Common Questions Asked of Our Incident Responders

Secureworks has assembled a collection of questions regularly asked of our experts by security leaders and practitioners just like you.

We thought we would share these along with our responses. Sometimes, it is nice to see what your counterparts in other organizations are asking.

1. What are some of the common gaps you see with Cybersecurity Incident Response Plans (CIRP) at organizations?

Your CIRP may be in trouble if it:

- Has not been tested
- Is lacking subject matter or sufficient detail
  - Roles and responsibilities are vague
  - Not appropriately integrated with other plans and processes, such as Business Continuity/Disaster Recovery/Crisis Management Plan
  - Not clearly articulated how a third-party vendor will be utilized
  - SLAs for third-party vendors are missing or vague
  - Lacks templates for critical communications
- Is lacking organizational support and buy-in
  - Plan sponsor lacks appropriate authority (e.g., Executive Leadership Team, CIO, CTO, CISO)
  - Incident stakeholders do not know the plan exists
  - Was developed unilaterally by a single business unit
  - Roles and responsibilities for non-technical teams are vague
- Is not maintained
  - Lessons learned are not captured after incidents and exercises and followed through
  - Missing/outdated contact information for teams/individuals with assigned roles or responsibilities
  - Contract terms for third-party vendors are unknown or not defined

2. So what are the key elements of an incident response plan?

Being prepared for a security incident can be the difference between finding calm in the face of the storm and total mayhem. To get it right, you need a CIRP built and maintained around several key ideas.

System and Information Classification Guidelines:

Having a systematic method to rapidly identify the level of importance of affected assets is critical to executing an appropriate level of response to an incident. System and Information Classifications are used as elements in assigning incident priority, assessing risk severity, scoping escalation, identifying stakeholders to notify, and deciding best course of action for containment, eradication and recovery.

Incident Response

The Secureworks Incident Response practice provides comprehensive and accredited Incident Response capabilities to enable you to prepare for and respond to a wide range of cyber threat scenarios and mitigate cyber incidents efficiently and effectively. Leveraging the latest proprietary Threat Intelligence and purpose-built technologies enriched with years of cyber-attack and threat group data, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents.

Incident Prioritization:

Not all incidents are equal. It is important your organization's reaction to an incident is appropriate, relative to the threats and importance of the assets involved. Incident Priority is an important consideration when triaging incidents, ensuring effective use of the limited resources available to most incident response teams. Incident Priority is more than just a defined threat model or list of possible incident types with an assigned level of priority. It requires an understanding of the underlying assets involved, the potential risk to those assets, and potential risks to the business those assets support. Defining Incident Priority requires the use of the classification guidelines mentioned above, as well as defined taxonomies for incidents, threats, impact and urgency.

Defining and Enabling the Response Team:

It is critical that responders to an incident quickly identify resources to address specific authorities and capabilities. Roles and responsibilities start with a definition of the Computer Security Incident Response Team (CSIRT) structure, which is generally defined as the Senior Leadership, Core, Extended and External teams. It is necessary to incorporate the whole organization, not just the technology and security groups. The plan builds on that structure to assign specific roles and responsibilities to groups like Legal, Finance, Public Relations, Communications and Human Resources. Additionally, these roles and responsibilities are used in the creation of the notification and escalation processes, organizing the communications plan, setting the response operational tempo, and specifying which role performs an activity or owns responsibility to make a decision. A subset of activities would include declaring an incident, engaging outside counsel, working with law enforcement, managing e-discovery, conducting forensics and maintaining custody of potential evidence. Similarly, a subset of decisions would include when to segregate a section of the network, remove a critical system from service, rebuild a system vs. preserve for analysis, and when to engage a third-party vendor for support.

Specific Response Processes:
Identifying team members and their roles and responsibilities is important, but the next step is to establish a common process that is both predictable and repeatable.

These processes can vary from a lightweight checklist to a detailed playbook. They generally cover the "what" needs to happen and should be created for each major incident type. Although these processes are not a "one-size-fits-all" proposition, the general thought process and steps carried out should be similar, regardless of the size and scope of the incident. Documenting these processes will ensure the appropriate steps are considered and carried out as necessary.

Incident Guides (identifying "what" needs to happen) differ from Standard Operating Procedures (SOPs) identifying "how" to do something. It is not uncommon to refer to SOPs in Incident Guides. Incident Guides should be constructed for each major incident type, focused on directing the response team to assign tasks to a team or individual.

Validating a CIRP:
Like backing up your data, the only way to know if a CIRP will work is to test it, either in an exercise or during an incident. Also like backups, it is best to assume your CIRP will not work sufficiently if it has not been tested.

When you have all of these elements in place, you can answer the inevitable question from leadership: "I saw another data breach in the news. Are we ready if this happens to us?"

3. How do you involve leadership in the response process?

There are many benefits to having a CIRP, but the overall intent is to improve coordination and decision making while limiting or avoiding damage during an incident. Effective coordination during an incident will span a number of internal groups, as well as external groups (primary vendors, law enforcement, external counsel, insurance brokers and forensics experts). A CIRP will assist in maintaining the relationships between various groups, setting expectations and guiding communications protocols, clearly articulate activities between the groups, and encourage participation during CIRP testing.

It is a fact that incidents interrupt normal operations. They require immediate attention and often swift decision making in order to limit impact to affected business operations. Understanding who has the authority to make a decision and who has the responsibility to execute that decision allows the CSIRT to focus on the technical issues of response. Additionally, once responsibility is assigned, that team or individual can begin building and socializing step-by-step procedures to execute the responsibility, further improving coordination.

The damages caused by a cybersecurity incident can be measured in many ways; hours of effort required to respond and remediate, period of service outage, payment withheld for not meeting an SLA, loss of consumer confidence, a reduction in stock price (if publicly traded), and fines (if regulated). Sometimes damages will include the costs of external support to respond and the cost of ensuing litigation(s). A CIRP can reduce damages by guiding an organization's technical and non-technical response efforts, lowering the risk of the incident escalating, meeting a regulatory mandate, and demonstrating due diligence.

4. How do I know my logging strategy is effective?

Great question. The failure of a logging strategy is a key reason many organizations cannot figure out what happened after a breach. In many cases, you already should have a logging strategy mandated by compliance standards such as PCI-DSS. In general, you should be able to have easy access to network perimeter logs and system logs, and put them in a centralized spot where they can be reviewed.

Generally, there are a few things we always like to see. First, we like to see data on logins and logoffs (security event logs) dating back at least three months, even longer, if feasible. Second, we also like the recording of remote accesses to systems that include date and time, source IP addresses, user account and other context (such as successful logon and failed logons). Finally, Web logs are also important, as are firewall, NetFlow and AV logs.

There is such a thing as too much collecting, however. For example, a recent client was collecting all the firewall activity within their servers' security event logs. The data was so extensive that it rolled over every 45 minutes. As a result when we investigated an intrusion for them and wanted to look at network logins – the number one useful thing security event logs contain – the data was worthless because we only had 45 minutes worth of data.

5. What are the top 3 mistakes you see organizations making when responding to incidents?

A general lack of planning can cause the most problems when a breach occurs and an organization has to respond. First, from our experiences, organizations with dispersed offices and infrastructure can lack centralized control of its security infrastructure. This decentralized approach can undermine any effective response, as roles, responsibilities and policies are not clearly defined or understood across the organization. Second, most organizations lack an up-to-date and tested incident response plan. We commonly find IR plans that are not current, are incomplete and/or have not been tested. Third, organizations do not capture sufficient logs, making forensics more time consuming and less conclusive. Organizations need to collect and centrally store its Active Directory, DHCP, Firewall, DNS and other logs for at least one year. Having access at your fingertips makes the job of the Forensic Analyst much easier.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.