Justifying a Computer Incident Response Plan

How a CIRP Can Pay for Itself Many Times Over, and Best Practices for Creating One

Contents

Survey: Effective Response Can Save an Average of $1.2 Million Per Data Breach ............................................. 1
What Is in a Computer Incident Response Plan? ................................................................. 2
How Can a CIRP Reduce the Costs of Cyberattacks? ......................................................... 2
Why Incident Response Is So Challenging ........................................................................ 4
Best Practices for Creating a CIRP .................................................................................... 4
How Dell SecureWorks Can Help ...................................................................................... 5

Survey: Effective Response Can Save an Average of $1.2 Million Per Data Breach

Companies that respond effectively and expertly to a data breach save a lot of money — as much as $41 for every record exposed, according to the Ponemon Institute’s 2011 Cost of Data Breach Study. That works out to $1.2 million for the average data breach in the survey (28,349 records).1

Information security experts point out that post-incident response actions can be just as important as pre-incident preventative measures. According to ISACA, “Recent events have demonstrated that while it is important for enterprises to have preventative measures in place to avoid security incidents, it is equally important that there be a robust, practiced response should an incident occur. An enterprise’s ability to detect, react and respond to security incidents in a fast, planned and coordinated fashion is important to the resilience and success of the enterprise.”2

Brought to you compliments of:

Dell SecureWorks

©2013 Dell
What Is in a Computer Incident Response Plan?

A Computer Incident Response Plan (CIRP) describes all of the people, processes and resources needed to detect, respond to and recover from cyberattacks and data breaches.

A CIRP can take many forms, but typically it includes at least four sections:

**Preparation and planning**
Preparation and planning should include acquiring management support; creating policies; identifying a Computer Incident Response Team (CIRT); acquiring incident analysis and communications tools; clarifying roles and responsibilities; conducting risk assessments; reviewing IT and security capabilities in areas such as patch management, malware protection and host and network security; creating policies, procedures and checklists (including communications plans); running drills for IT security, operations and support staff; and conducting security awareness training for all employees.

**Detection and analysis**
Detection and analysis usually include plans and procedures for monitoring systems and logs; detecting, categorizing and prioritizing security events and incidents; conducting forensic investigations of malware and attack behaviors; determining the identity, motives and goals of attackers; documenting the course and impact of attacks; and preserving evidence.

**Containment and recovery**
Plans for containment and recovery typically cover blocking any further attack activities; preventing information from being exfiltrated from the organization; eliminating all traces of malware and malicious code; communicating incident status and consequences to executive management, employees, customers, business partners, regulators and media (if appropriate); cleaning and recovering systems and data; and restoring normal operations.

**Post-incident analysis and remediation**
Analysis and remediation usually include conducting postmortem analyses (“Exactly what happened?” “How well did we respond?”), compiling metrics (for example, mean time to discovery and cost of recovery), documenting the incident and response for auditors and outside parties, and taking steps to prevent recurrences of the same types of incidents.

Resources and guidelines for creating a CIRP are available online from sources such as ISACA, the National Institute of Standards and Technology (NIST), Dell SecureWorks and TechTarget SearchSecurity.

How Can a CIRP Reduce the Costs of Cyberattacks?

**Shortening the discovery-to-containment cycle**
A CIRP helps companies reduce costs by shortening the duration of attacks. For many types of attacks, the costs to the business are proportional to the length. As an attack goes on:

- More systems with confidential files are identified and compromised.
- More customer records, employee files and intellectual property are exfiltrated.
• More sales and employee work hours are lost when websites, computers and IT services are disabled.

• More systems need to be cleaned and restored to operation.

These factors can lead to greater damage to reputation and brand equity, larger legal and regulatory fees, higher breach notification costs and slower response to other IT priorities.

And cyberattacks take longer to contain than most people imagine — an average of 24 days, according to one survey.

An effective CIRP will reduce these costs by shortening the discovery-to-containment cycle and more quickly restoring normal operations. It ensures that the organization has the team, skills, tools and policies in place to:

• Assemble log data.
• Conduct forensic investigations.
• Find and remove all malware.
• Stop further damage.
• Communicate appropriately with all stakeholders.
• Recover systems and restore operations quickly.

**Preventing attacks through analysis and planning**

President Dwight Eisenhower once said, “Planning is everything.” The same can be said for CIRPs. Deficiencies in systems, policies and processes are identified in the preparation and planning phase of the CIRP, through risk assessments, evaluations of security capabilities and consideration of the security skills needed on the CIRT. Other vulnerabilities are pinpointed during the postmortems and “lessons learned” sessions that are held as part of the post-incident analysis and remediation phase.

The planning process and “lessons learned” sessions often uncover issues like:

• Inadequate security event monitoring.
• Insufficient segregation of sensitive systems.
• Missing security controls (for example, dual administrator accounts).
• Unpatched desktop software.
• Insufficient email scanning.
• Lack of an Internet acceptable-use policy and tools to enforce it.

• Lack of malware analysis and forensic investigation skills (or dependence on a single individual).

• Lack of communication and diplomatic skills.

Remedying these deficiencies in a timely manner can protect against attacks in the future and limit data breach costs.

Why Incident Response Is So Challenging

Today's attacks are very difficult to detect and contain for the following reasons:

• Many specialized skills are needed to identify and remediate sophisticated, cutting-edge attacks such as advanced persistent threats, social engineering and polymorphic malware.

• Incident response involves many people beyond the IT security staff, including IT operations, help desk staff, legal and compliance officials, human resources, public relations, top executives and others.

• Once the initial symptoms are discovered, security breaches often create an atmosphere of chaos, urgency and exhaustion that tax the resources of participants and lead to errors.

Best Practices for Creating a CIRP

Build the right team: An effective CIRT requires individuals with specialized skills and experience. Organizations should take an inventory of trained personnel. They should also determine areas where they do not have the appropriate levels of expertise in-house or rely on a single key individual, so that external incident response resources may be needed. Required skills are listed in the CERT document, “Staffing Your Computer Incident Response Team — What Basic Skills are Needed.”

Identify priorities: If a company is covered by PCI DSS payment card standards, HIPAA healthcare regulations or other similar standards, then safeguarding protected data is critical. If a company is an online merchant or depends heavily on its website, then restoring the website in the minimum time may be imperative. If employee productivity is critical, then keeping business processes running may be the top priority.

Create a thorough but flexible plan: The CIRP needs to be detailed, but also flexible enough to address unforeseen events. Therefore, it should include specific plans for high-risk attack types and generic plans for the unforeseen. The latter is especially important to respond to targeted attacks and exploits involving sustained and organized efforts and multiple threat vectors.

Include all affected groups: The plan should spell out the roles and responsibilities of all participants and affected parties — not just IT security, but also IT operations, employee and customer support, legal and compliance officials, human resources, public relations and top executives.
Review and test: Reviews and tests greatly improve the effectiveness of plans, and ensure that all team members understand their responsibilities and can coordinate their activities. For example, table-top tests and war games with participants from many departments can uncover critical issues that might not be apparent to the IT staff, such as compliance with obscure regulations, contractual obligations to customers, and confidential documents stored on shared servers.

Get an outside opinion: A company that specializes in incident response can provide security personnel and executive leadership with critical insights and experience. Specialized expertise ensures that the organization will have a CIRP in place that is comprehensive, incorporates proven best practices and will work when it is most needed.

How Dell SecureWorks Can Help

Dell SecureWorks can help organizations:

- Establish an end-to-end incident response capability to address even the most sophisticated threats.
- Develop a sound CIRP based on industry best practices.
- Reduce vulnerabilities by identifying risks and gaps in security practices.
- Respond more quickly and effectively to attacks as they occur.
- Reduce the duration and disruption of security breaches and incidents.
- Minimize damage, recover compromised data and preserve evidence for legal action.
- Return to a normal state after a serious security breach.

The advantages of working with Dell SecureWorks include:

- Dedicated specialists who work on only incident response engagements.
- A wide range of skills in malware identification, forensics, malware reverse engineering, and use of intrusion prevention and other security technologies.
- Extensive experience with the nontechnical aspects of handling incidents under crisis conditions, including coordinating resources and handling communications with all stakeholders.
- Extensive lab facilities set up for incident response and forensics activities.
- Extensive threat intelligence sharing through the Dell SecureWorks Counter Threat Unit.
- Service-level agreements that ensure that skilled personnel will be on-site in as little as 24 hours.
- Up-to-the-minute visibility into new threats and experience as the trusted security partner to more than 3,000 customers.
Incident Response Retainer Service

Dell SecureWorks also offers an Incident Response Retainer service, which has proven to save many organizations substantial amounts of time and money. The advantages of a retainer agreement are:

- There is no delay for negotiation or contract signing during the course of an incident (activities that can add hours or even days to the duration of a breach).
- Dell SecureWorks specialists are guaranteed to be available to work on your incident and can be on-site in as little as 24 hours.
- Dell SecureWorks team members are equipped with the information and contacts they need to become effective immediately upon notification of an incident.
- Professional service hourly rates are locked in at a discounted level.

The Incident Response Retainer service helps organizations prevent cyberattacks through better analysis and planning, and reduces the costs of attacks that do occur by shortening the discovery-to-containment cycle.

To learn more about Dell SecureWorks, visit www.secureworks.com.

---

1 Ponemon Institute: **2011 Cost of Data Breach Study**, March 2012. The study found that the average cost of a data breach for companies that hired consultants to assist in data breach response and remediation was $188 per record, versus $209 for companies that did not. The cost per record included costs for detection and forensics, crisis team management and communications with executive management, lost business, legal expenditures, and notification of affected parties. The average total cost of a breach was $5.5 million.

2 ISACA: **Incident Management and Response** white paper, March 2012.