bsi.

...making excellence a habit.™

Determining the effectiveness of an incident response plan

Study based on lessons learned from a real life incident

A whitepaper

Executive summary

This whitepaper aims to provide an insight on how to assess the effectiveness of an incident response plan, based on our experience in mitigating incidents and lessons learned from a real life case study.

Business challenges

It is not possible to completely eliminate the occurrence of incidents and therefore it is important to ensure highly effective response plans are in place to react should an incident occur. An Incident Response Plan should be formalized and needs to cover a complete set of response areas relevant to the affected institution in order to:

- Allow smooth execution
- Minimize business impact
- Minimize the likelihood of incident reoccurrence

Measuring the effectiveness of the incident response plan poses a challenge to enterprises and sometimes is only looked at after an incident happens.

Case study - real life incident

Incident background

We were engaged to provide incident response support during a malware outbreak on a company's internal network. The outbreak was pervasive and resulted in disruption to key service channels, particularly email which was a vital customer support channel.

The origin of the malware was tracked back to an external email attachment. The mail was originally blocked at the perimeter as it contained attributes determined as potentially harmful. The intended recipient was notified about the email being blocked and decided to release it from quarantine, even though he was not expecting to receive any such document from the unknown sender.

The user opened the attached word document which subsequently executed the embedded malware.

Once executed, the malware propagated throughout the network via the local email client. All address book contacts were targeted with the infected file. As a result of the increase of email activity, the mail server CPU spiked to 100% and caused an outage.

At this point the email outage was the only indicator that a virus infection had occurred and it was sufficient enough to draw the attention of the business. Without this indicator, it is likely that the malware would have gone unnoticed. The malware itself was a relatively benign malware, effectively a "dropper", which could be further used to pull down malware depending on the command and controller requirements. We deployed an onsite Network IDS and were able to identify the command and control servers being polled and ultimately block the traffic and further other infected hosts.

The company deployed Anti-Virus (AV) software on all workstations, which in the case of this particular incident proved to be of a limited use. Although the malware type was generally known, their particular AV engine was not detecting this new malware variant. A number of the leading AV vendors did not have the signature.

The Incident Response (IR) process

The incident response process can be typically divided into the following six stages:

- Prepare
- Identify
- Contain
- Eradicate
- Restore
- Lessons Learnt

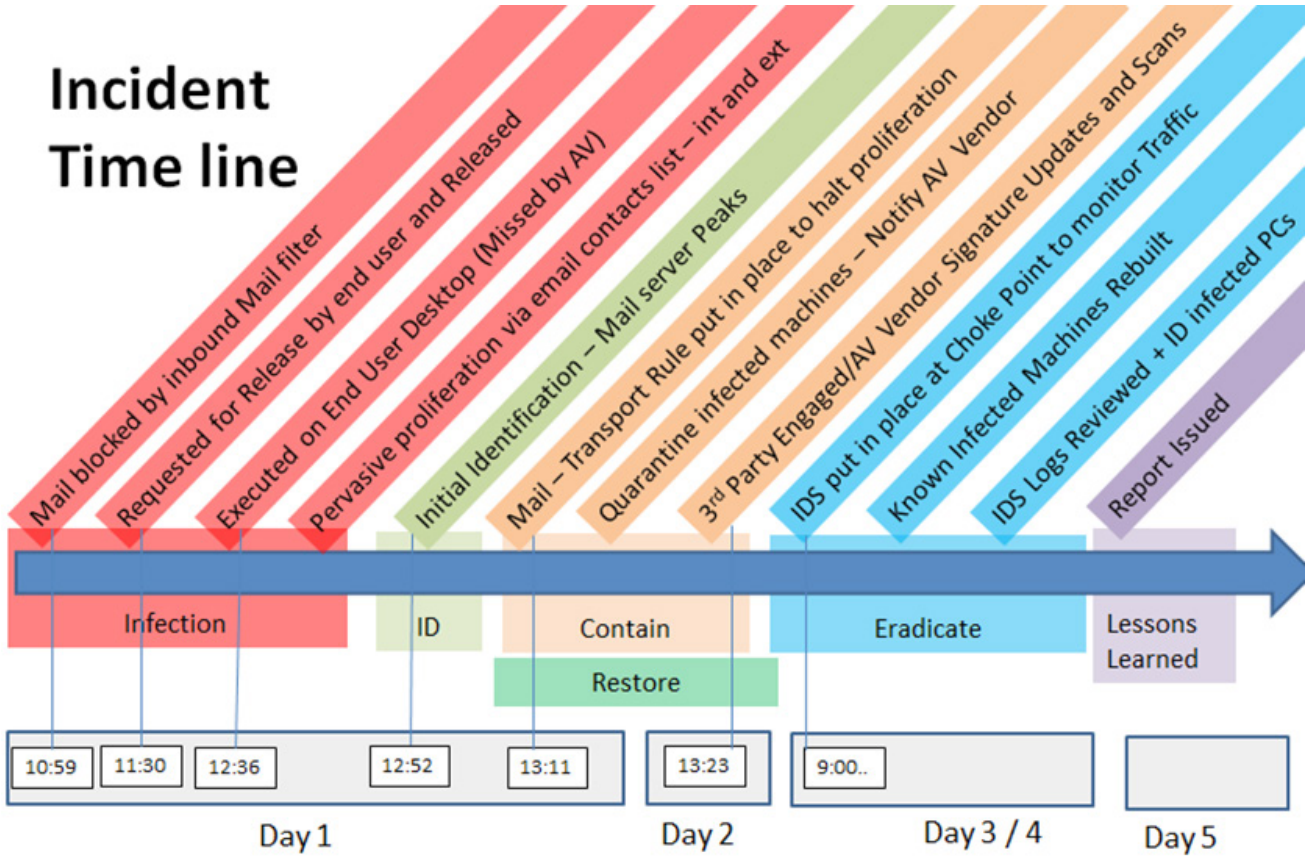
The diagram below shows how the last five stages map into our case study incident response process.

During the engagement it was discovered that key security controls were missing:

- No formal incident response preparation
- Lack of adequate information security related user awareness training
- Inappropriate tools and processes for blocking inbound mail – all zips being blocked lead to "warning fatigue" and users release zips as standard
- Lack of security incident response training and testing
- Inconsistent management of anti-virus end point protection across the estate
- Systems identified without any anti-virus installed
- Limited inbound and outbound network AV
- Lack of adequate logging and monitoring

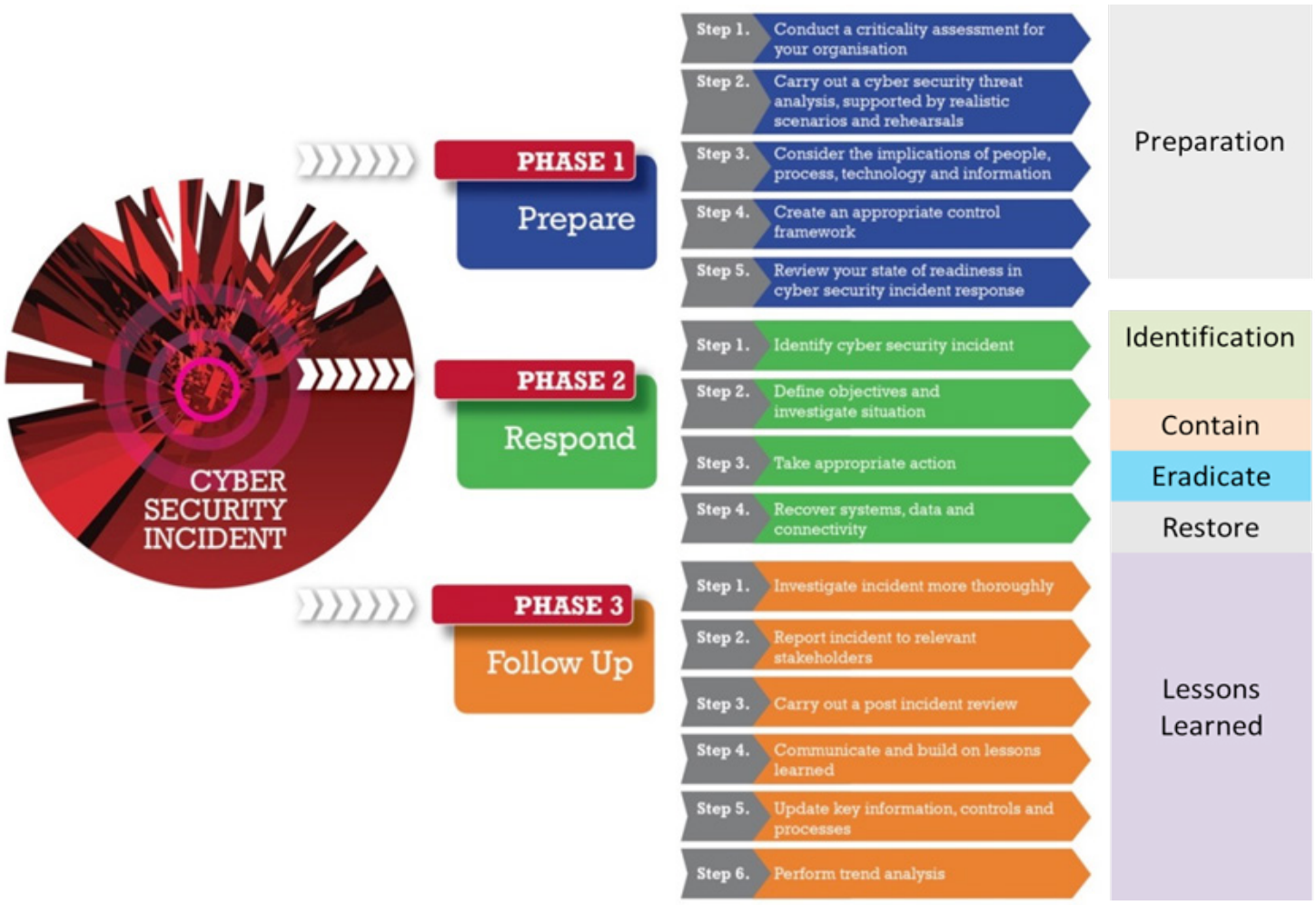
Over the course of the IR process, we helped contain the incident from further proliferation to other (unaffected) environments and operations were restored.

Subsequent to the containment and eradication of the incident, the root cause of the incident was identified and lessons learned sessions were conducted to ensure that the likelihood of a reoccurrence was reduced. This included an assessment of the effectiveness of the incident response process in the organization and ultimately the implementation of new processes, procedures and systems to ensure effective response.



Validating the effectiveness of an incident response process

CREST – a non-profit organization, providing assurance over the quality of services offered by security firms – has developed a well-defined model for assessing the maturity of each of the six incident response stages.



Preparation

Key controls to check when assessing effectiveness of this IR stage are:

- Analyse the following elements during periodical facilitated incident simulation tests:
  - Incident response timeline template
  - Contact details of critical stakeholders: internal and external investigators, technical specialists, suppliers, legal resources, human resources, public relations and business management, external regulatory bodies
  - Incident analysis resources: such as port lists; packet sniffers and protocol analysers; documentation: IDS, SIEM: network diagrams; asset inventory
- Prepare incident response toolkit which would include:
  - Forensic imaging tools

- Physical tools (e.g. screw drivers, wire cutters, torches, gloves, cameras etc.)

- Look for documented evidence of the above being in place during an audit

Identification

Ensure that systems and monitoring are in place to cover the following indicators of compromise:

- Unusual outbound network traffic
- New admin users created
- Anomalies in privileged user account activity (first logon to a system)
- Geographical irregularities (non-standard login attempts)
- Increased database read Volume (database dump)
- Large numbers of requests for the same file
- Suspicious registry or system file changes
- Unexpected patching
- Signs of DDoS activity

Contain

Review containment strategies to ensure that the following types of actions are covered:

- Defined course of action based on potential impact of the incidents
- Blocking (and logging) of unauthorized access
- Blocking malware sources (e.g. email addresses, IP addresses and websites)
- Closing particular ports and mail servers
- Firewall filtering
- Relocating website home pages
- Isolating systems on the network
- Taking back-ups
- Turn systems off

Eradicate

Key controls to check when assessing effectiveness of this IR stage are:

- Eliminate the cause of the incident – this stage may overlap with the containment stage. Aim is to eradicate the cause, the actual incident and the compromise itself
- Verify eradication e.g. by monitoring traffic and reviewing critical logs
- Check if eradication steps include such elements as:
  - Removing the attack from the network
  - Deleting malware
  - Disabling breached user accounts
  - Identifying vulnerabilities that were exploited
  - Mitigating vulnerabilities that were exploited
  - Is there a formal process for handling evidence when dealing with an incident?
  - Do you take steps to preserve evidence when dealing with an incident?
- Do processes for handling evidence include:
  - Allowing for admissibility of evidence
  - Complying with relevant laws?

Restore

Key controls to check when assessing effectiveness of this IR stage are:

- Recovery plans should be reviewed to determine whether the following are in place. The following are the core tasks in the restore stage:
  - Prioritize system recovery
  - Restore data from back-ups
  - Update / notify stakeholders
  - Address similar vulnerabilities on the network
  - Complete incident report
- Does your recovery plan cover basic recovery techniques, including:
  - Rebuilding infected systems (often from known 'clean' sources) in a prioritized manner?
  - Reconnecting networks?
  - Restoring, recreating or correcting information?
  - Documenting changes made to the infrastructure?
  - Dealing with parts of your systems or networks that cannot be recovered?
- Do you validate that systems are operating normally by:
  - Carrying out an independent penetration test of

the affected systems?

- Undertaking a security controls assessment?
- Once systems have been recovered and controls have been tested, do you provide stakeholders with a brief summary of what took place?
- Do you brief stakeholders within a day or so of the event?

Lessons learned

Plans should be reviewed to determine whether the following tasks are in place:

- Complete post incident review - do your post incident reviews include analysing the incident management process to determine:
  - How quickly actions were taken to identify, respond to and recover from the incident
  - How long attackers were in systems before detection
  - What actions attackers took and planned to take
  - The level of protection maintained over critical systems and confidential information during the incident
  - How well staff and management performed in dealing with the incident
  - If all key discussions and decisions conducted during the eradication event were well documented
  - The effectiveness of procedures
  - If any steps or actions taken might have inhibited the recovery
- Identify lessons learned - do you identify lessons learned from security incidents and ensure they are:
  - Formally documented
  - Communicated to relevant stakeholders
  - Built upon in the form of tangible actions
  - Used to share both key issues and good practice across all areas of the business, not just within IT and cybersecurity teams
- Update IR plans and procedures - following a security incident, were the following updated:
  - Security incident management methodologies or processes
  - Security incident response plan
  - Management controls (e.g. training and awareness)
  - Technical controls (e.g. patching, configuring system logs, and use of intrusion prevention / detection tools)
  - Roles and responsibilities for handling

Conclusion

Although it is not possible to fully prepare for unknown future incidents, there are elements of an incident response process which require preparation, to allow effective incident mitigation.

To name just two of these elements:

- Detection capabilities need to be developed to allow early identification of the issue before it becomes a problem. In our case study incident, these capabilities were limited and the problem was detected only when mail services were affected
- Key stakeholders have to be defined and communication procedures must be in place to allow effective decision making while keeping incident-related information confidential. An incident response simulation exercise is an extremely valuable tool to identify where gaps may be present in your response process.

The bottom line is that an incident response plan not only needs to be formally defined, but must be periodically assessed to ensure it is still effective.

Applying a well-defined and mature incident response framework, like the one developed by CREST helps covering all important aspects of such an assessment.

Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

Find out more

Call: +1 800 862 4977

Visit: bsigroup.com/cyber-us

bsi.