Incident Response Models

As global regulators start to tentatively embrace the concept of cyberresilience, it is clear that there has been a significant change in the way that cyberattacks are perceived. Underpinned by countless data breaches involving some of the biggest names in industry, organizations are waking up to the fact that it is no longer if they will be attacked, but when.

In 2018, Symantec cited a 13 percent increase in reported vulnerabilities, a 54 percent increase in mobile malware variants and a 600 percent increase in attacks against Internet of Things (IoT) devices.[1] These statistics, among others, lead to the conclusion that the threats faced by enterprises have become more diverse and more numerous.

Against this backdrop, organizations are being advised to develop their incident response (IR) capabilities so that they can effectively respond to these kinds of incidents. "Incident," in the context of computer security, is defined as "an adverse event in an information system and/or network."[2] Recent examples have shown that incidents can have far-reaching impacts on organizations.

Here, IR is defined as "the mitigation of violations of security policies and recommended practice."[3] COBIT® 2019 states that the aim of IR is to "provide timely and effective response to...and resolution of all types of incidents," with the ultimate goal of supporting the delivery of information and technology services in line with business requirements.[4]

Established Models for IR

While it is clear that IR is an important aspect of wider cyberoperations, it is important to ensure that IR capabilities are applied systematically and consistently. Several authoritative governmental and industry bodies have proposed IR models that organizations can use to establish and mature their own IR capabilities. An overview and analysis of the models proposed by the US National Institute of Standards and Technology (NIST), ISACA® and CREST follows.

NIST

In 2012, NIST released a revision of Special Publication (SP) 800-61 that provides guidance on how organizations should respond to computer security incidents.[5] It outlines how organizations can establish and mature their IR capabilities and provides detailed guidance on team structures, staffing models, tools and other services IR teams can offer the wider enterprise. SP 800-61 also proposes a life cycle that breaks the IR process into four phases:

1. Preparation
2. Detection and analysis
3. Containment, eradication and recovery
4. Postincident activity

The document describes key activities within each phase but emphasizes that these phases should not be viewed as linear. NIST acknowledges that IR teams will likely move between phases several times during an incident.

Cameron Young, CCP, CCSP, CISSP, M.Inst.ISP
Is a cybersecurity professional who has spent the last few years working in senior security officer roles in the UK insurance sector, having transitioned from defense. Among other highlights, Young helped support the incident response activity associated with a highly publicized security breach at a large telecommunications company. Young currently works as the head of security management and assurance at Legal and General, one of Europe's largest insurance and asset management groups.

> ONE UNIQUE ASPECT OF THE CREST MODEL IS AN ACKNOWLEDGMENT THAT, FOR SOME ORGANIZATIONS, OUTSOURCING ALL OR PART OF THE IR CAPABILITY IS THE MOST APPROPRIATE COURSE OF ACTION.

In addition, SP 800-61 stresses the importance of coordination and information sharing with internal and external stakeholder groups to "strengthen an organisation's ability to effectively respond to...incidents."[6] SP 800-61 integrates with a number of other NIST guidance documents, particularly SP 800-86,[7] which articulates how organizations can incorporate digital forensic techniques into IR processes, and NIST's wider Cybersecurity Framework (CSF).[8] SP 800-61 provides a holistic framework for IR, but it is deliberately tool- and platform-agnostic and highly abstract so that it is applicable to organizations at varying levels of maturity.

ISACA

Management Objective DSS02 of the COBIT® 2019 IT governance framework, published by ISACA, deals with managed service requests and incidents.[9] From an incident perspective, the guidance states that the purpose of IR is, ultimately, to support the delivery of information and technology (I&T) services. The COBIT® model does not include a life cycle, but it describes the management processes that should be in place for IR and the mechanisms required to assess the maturity of those processes.

Each process features a number of activities, and the Capability Maturity Model Integration (CMMI) level associated with each one is indicated. This intrinsic link between the COBIT and CMMI models allows organizations to use COBIT to assess the current maturity of their IR capabilities and to identify processes and associated activities that should be established or matured to meet target maturity levels.

In addition to processes and associated activities, the COBIT framework provides sample metrics, references to more detailed guidance, a view of roles and responsibilities, and suggested inputs and outputs for each activity.

CREST

In 2013, CREST published a guide for cybersecurity IR that outlines a model with three high-level phases.[10] The guide focuses on providing practical advice, but the model includes a number of detailed steps associated with each phase of the life cycle. Although the CREST model may seem distinct from the others described, a deeper look at the "respond" phase of the model reveals that it is based on the guidance contained in NIST SP 800-61 and that identification, containment, eradication and recovery are included as individual steps in this phase.

A key feature of the CREST model is a five-point maturity scale as part of the "preparation" phase. The guide does not specifically refer to the CMMI model, but CREST's five-point system uses similar labels for the various maturity levels. CREST suggests that identifying the current maturity level is important so that enterprises can ensure that they are maintaining an appropriate IR capability in line with that of their industry peers.

One unique aspect of the CREST model is an acknowledgment that, for some organizations, outsourcing all or part of the IR capability is the most appropriate course of action. In fact, CREST has published a guide for the selection of cybersecurity IR suppliers to help organizations identify which processes and activities to outsource, establish supplier selection criteria and, subsequently, appoint an IR supplier.[11]

Conclusion and Recommendations

NIST and CREST have proposed similar IR life cycle models, highlighting the general consensus that an IR life cycle should include phases focused on identification, response and lessons learned. These models also highlight the importance of ensuring that the IR capability is completely prepared for an incident, and they both recommend that organizations hold regular lesson-learned sessions following an incident to identify opportunities for continuous improvement.

COBIT can be used by organizations to understand the maturity associated with IR processes. Not all organizations need a full IR capability, but using CMMI maturity levels enables them to identify their current maturity and conduct gap analysis against the ideal target state. CREST also suggests using maturity levels in this way.

All the models reviewed highlight the fact that IR capabilities have multiple dependencies such as management buy-in and support, access to systems, data, facilities, and business stakeholders from a range of internal teams. It is important that organizations understand and manage these dependencies to ensure that the IR capability is effective. In addition to the core IR model, the NIST and ISACA models highlight the IR team's role in wider cyberoperations.

Finally, the CREST guidance highlights a number of challenges that could significantly hinder immature IR capabilities. Understanding and making appropriate allowances for these challenges will ultimately allow the organization to establish a mature, systematic and consistent IR model. Based on these conclusions, it is recommended that organizations do the following:

- Review current IR policies and processes to accommodate the good practices outlined in NIST SP 800-61, COBIT 2019 and the CREST guidelines.
- Ensure that IR teams are fully prepared to conduct IR activities based on the guidance contained in SP 800-61.
- Ensure that the processes outlined in SP 800-61 and COBIT 2019 are established and operated.
- Consider whether outsourcing all or part of the IR capability would be appropriate and cost-effective.
- Use COBIT's integrated CMMI maturity levels to identify the current maturity of IR processes, and then determine how to achieve the target CMMI maturity level.
- Understand and manage the dependencies of IR.
- Ensure that the IR capability is fully embedded in wider cyberoperation capabilities.
- Consider having IR teams undertake proactive threat-hunting duties when they are not responding to or preparing for an incident.

Endnotes

1 Symantec, *2018 Internet Security Threat Report*, *https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf*
2 Kral, P.; *Incident Handler's Handbook*, SANS Institute, USA, 2012, *https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901*
3 National Institute of Standards and Technology, *Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide*, USA, 2012, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*
4 ISACA®, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx*
5 *Op cit* National Institute of Standards and Technology
6 *Ibid*.
7 National Institute of Standards and Technology, *Special Publication 800-86: Guide to Integrating Forensics Into IR*, USA, 2006, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf*
8 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, vol. 1, USA, 2018, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*
9 *Op cit* ISACA
10 CREST, *Cyber Security IR Guide*, United Kingdom, 2013, *https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf*
11 CREST, *Cyber Security IR Supplier Selection Guide*, United Kingdom, 2013, *https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Supplier-Selection-Guide.pdf*

Enjoying this article?

- Read *COBIT® 2019 Framework: Governance and Management Objectives*. *www.isaca.org/resources/cobit*
- Learn more about, discuss and collaborate on COBIT and Frameworks in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*