Auditing the Crown Jewels From a Cyberrisk Perspective

Auditing standards require auditors to produce a documented risk-based audit plan,[1] taking into account input from senior management and the board. Cyberrisk is one of the top risk scenarios about which boards are concerned[2, 3] and should, therefore, receive significant focus during audit planning as one of the higher priorities for auditors.[4] Emerging risk (including cyber) and the evolution of the risk landscape is constant, resulting in numerous complications in the audit planning process that could lead to risk not being appropriately addressed in the audit plan. Additionally, executing on the audit plan can be tedious and manual in many cases, leading to limited coverage of key risk areas.

In an article on practical cyberrisk management,[5] the author discusses the concepts of crown jewels, threat modeling, attack path mapping, the Cyber Kill Chain and data modeling, and how to apply each concept in cyberrisk management. The same concepts that apply to cyberrisk management can be applied to audit planning, both from an overall annual plan and a detailed audit plan perspective.

Management applies the crown jewel approach to determine which assets and processes are the most critical as an indication of where to design and implement controls. The auditor can apply the crown jewel approach to determine which assets and processes are the most critical and could have the most impact to the organization to guide where to focus audit efforts. Management uses threat modeling and attack-path mapping to determine what the most likely attacks are that the organization could expect and how the attacker would execute the attack to develop the appropriate controls for attack mitigation. The auditor can use threat modeling and attack-path mapping to assist with understanding where key controls are expected to exist; where they do not exist becomes the basis of control gap recommendations. The Cyber Kill Chain assists management with a logical analysis of how an attack would play out in various stages and where to implement controls. The Cyber Kill Chain can assist the auditor in ensuring that all the key controls to prevent and detect an attack in each of the stages are included in the audit plan.

Furthermore, if the testing of controls that mitigate these risk scenarios are automated as much as possible through building data models and using advanced techniques (e.g., robotic process automation [RPA]), the auditor can achieve superior coverage on the aspects that matter most.

Crown Jewels

Identifying crown jewels[6] indicates to the auditor what assets and processes are important. A skilled cyberauditor is a scarce resource and needs to focus on critical aspects such as ensuring that audit coverage and effort is prioritized on the assets and processes that can cause the greatest harm to the organization if compromised, and identifying opportunities where automation can be applied to audit continuously across the population and across the period under review. It is not possible to audit everything in an organization, and isolating the most critical assets and processes ensures that scarce audit resources are optimally applied. Crown jewels can be identified through an iterative process of workshops with management to identify a list of critical assets and supporting processes as indicated in **figure 1**. Crown jewels can differ from industry to industry. In some cases, crown jewels can be digital assets; in other cases, crown jewels may be a physical building or a manufacturing process. Depending on the size of the organization, the initial list could be many high-risk items. The final list of crown jewels should, however, be the most important subset of the high-risk items due to the high cost of applying specialized controls to crown jewels. The number could differ from

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2nVDXQR

Jaco Cloete, CISA, CRISC, CISM, CSX-P, CA, C|CISO, CISSP
Has 22 years of experience in cyberrisk management and auditing in the banking sector. He performed audits across all information technology and cyberdomains and served in both an external and internal audit capacity. In his current role, he is responsible for cyberstrategy, cyberpolicy, cyberrisk management, cyberresilience program management, red team testing, cyberscenario analysis, cyberthreat identification and modeling, and cybermetrics and reporting.

> THE FINAL LIST OF CROWN JEWELS SHOULD, HOWEVER, BE THE MOST IMPORTANT SUBSET OF THE HIGH-RISK ITEMS DUE TO THE HIGH COST OF APPLYING SPECIALIZED CONTROLS TO CROWN JEWELS.

organization to organization based on the resources that the organization is willing to allocate to management of the crown jewels. The list should be ranked from most critical to least critical. Examples of crown jewels include:

- A payment switch in a bank
- The Society for Worldwide Interbank Financial Telecommunication (SWIFT) environment that enables financial institutions worldwide to send and receive information about financial transactions
- A concentration of customer data
- A plant manufacturing control system

Audit effort should be applied starting at the top of the crown jewel list and moving down the list. The crown jewel list should be addressed on an annual basis at minimum, with subsequent items on the list addressed on a rotating basis as resources permit.

Threat Modeling/Attack-Path Mapping

Threat modeling and attack path mapping provide the auditor with insight into how an attack could potentially be performed against a crown jewel and who would most likely want to perform such an attack. This understanding assists the auditor with identifying the critical points where key controls should exist to detect or prevent the attack.

One example assumes that the control system that monitors the temperature of a manufacturing plant is a crown jewel in an organization and that unplanned downtime of the production unit will have catastrophic financial consequences to the organization. One attack path is to compromise a user through a malicious email, as depicted in **figure 2**. The email has an attachment that installs malware, which then creates a connection with the attacker's computer on the Internet. The attacker uses the persistent connection to move laterally on the internal network to compromise the workstation of an authorized user of the application that monitors and regulates the temperature of the production unit. Another attack path is to obtain credentials of the crown jewel user through a phishing email and log on to the user's workstation. Once the user's workstation is compromised, the attacker logs in to the temperature monitoring application and changes the temperature threshold to a dangerously high level. The effect is that the production unit overheats, the unit fails and it shuts down.

Figure 1—Crown Jewels

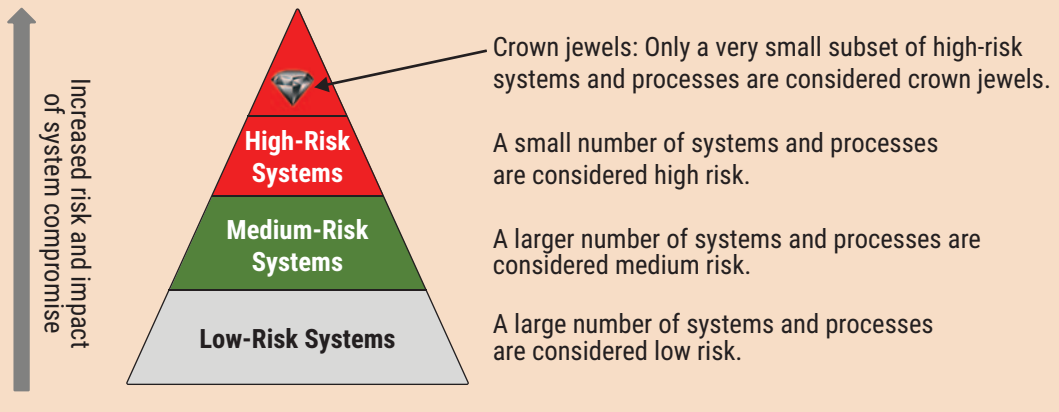
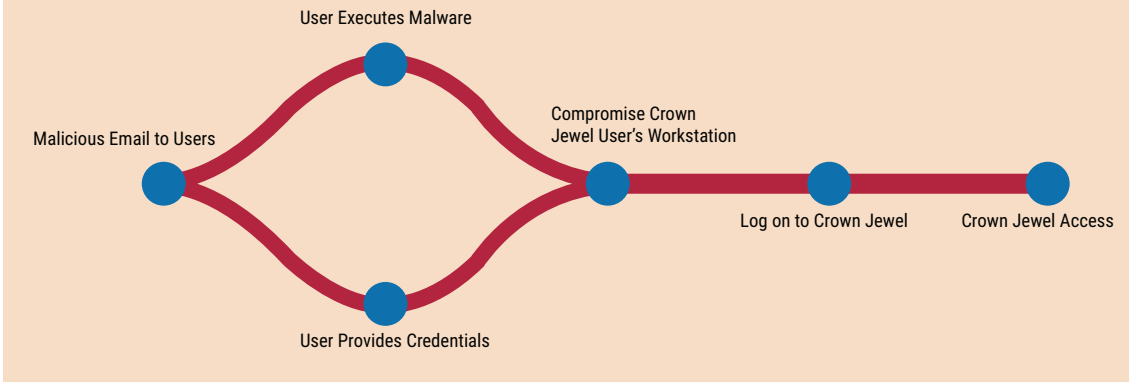


Figure 2—Cyber Kill Chain



There can be many valid attack paths, and these should be documented as comprehensively as possible, with validated attack paths receiving higher priority than theoretical attack paths. Attack path mappings are typically performed by cyberrisk management functions utilizing red teams that validate attack paths, and the outcomes of those tests inform the auditor.

Cyber Kill Chain

Utilizing the Cyber Kill Chain, developed by Lockheed Martin,[7] assists the auditor with identifying key controls that will prevent or detect a cyberattack along various stages of the attack and with focusing audit effort on these controls.

The Cyber Kill Chain depicts the stages that a cyberattack follows from reconnaissance to achieving the objective. Each attack path to the crown jewel can be overlaid onto the Cyber Kill Chain and, during each stage, key controls can be identified that will detect or prevent the attack. Examples of attack methods and controls are depicted in **figure 3**.

During the exploitation stage, the user could execute malware sent to him or her via a malicious email by clicking on the attachment. A key control in this stage is for the cyberteams to perform cyberawareness training to prevent users from clicking on suspicious attachments in emails and disclosing their credentials when asked for them by someone. Cyberawareness controls include phishing and vishing simulations, awareness videos, awareness presentations, awareness events, and compulsory awareness training.

During the command and control stage, the attacker establishes a connection to the command and control center on the Internet. A key control in this stage is for cyberteams to detect abnormal connections to suspicious domains on the Internet.

During the actions on the objectives phase, the attacker logs on to the target system and changes the temperature thresholds. A key control in this stage is for staff who log on to the temperature monitoring and control system to use two-factor authentication. In addition, the MITRE ATT&CK knowledge base[8] is an excellent source that the auditor can consult for a list of attack methods and key controls in various stages of a cyberattack.

> "THERE CAN BE MANY VALID ATTACK PATHS, AND THESE SHOULD BE DOCUMENTED AS COMPREHENSIVELY AS POSSIBLE, WITH VALIDATED ATTACK PATHS RECEIVING HIGHER PRIORITY THAN THEORETICAL ATTACK PATHS."

The key controls can be grouped into two types of controls: those that are pervasive in nature and those that are specific to a certain crown jewel. Pervasive controls are those controls that, if compromised, enable the attacker to successfully attack a wide range of crown jewels. Specific controls are those controls that relate to a specific crown jewel and need to be compromised for an

Enjoying this article?

- Read *Bridging the Digital Risk Gap. www.isaca.org/rims-when-worlds-collide*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 3—Examples of Attack Methods and Key Controls

Cyber Kill Chain Stage	Description of the Stage	Attack Method	Key Control
1. Reconnaissance	Attacker conducts research to understand which targets will enable him to meet his objectives.	Discover Internet scanning servers.	Detect scans against the Internet-facing IP addresses.
2. Weaponization	Attacker prepares the operation by creating a payload consisting of malware and an exploit.	Obtain weaponizer tools from the dark web.	Implement detection controls against weaponizer artifacts.
3. Delivery	Attacker launches the operation by delivering the malware to the user.	Send malware to the user via email for execution by the user.	Analyze delivery medium, e.g., sandbox execution of attachment.
4. Exploitation	Attacker gains access to the victim by exploiting a vulnerability.	Use of a zero-day exploit against the target or exploiting a human vulnerability.	Provide cyberawareness training to users not to click on links.
5. Installation	Attacker establishes a beachhead at the victim for persistent access.	Install a backdoor on the target system.	Utilize endpoint detection and response tools.
6. Command and control (C2)	Attacker remotely controls the target system through a communication channel.	Establish two-way channel to C2 infrastructure.	Detect anomalous domain connections.
7. Actions on objectives	Attacker achieves the mission goal through access on the target system.	Log on to target system to change thresholds.	Utilize two-factor authentication.

attack on that crown jewel to be successful. Grouping controls in this way assists the auditor in planning generic audits on pervasive controls and specific audits on crown jewels.

Examples of pervasive controls are the compromise of Active Directory and the domain, as these attacks feature in numerous attack paths and are relevant to many crown jewels. A compromise of Kerberos, for example, can lead to authentication to all applications that rely on this authentication mechanism, irrespective of the crown jewel and, similarly, a compromise of the domain password hashes can lead to the compromising of many user and system account passwords, irrespective of the crown jewel. A generic audit on the domain controls could be appropriate in this case.

Examples of specific controls in the SWIFT environment, on the other hand, are controls relating to the Left and Right Security Officers (LSO/RSO) or the secure zone, as they are specific to the compromise of the SWIFT crown jewel. In this case, it is appropriate to test those controls in a specific SWIFT audit.

Monitoring connections to suspicious domains on the Internet during the command and control phase of the Cyber Kill Chain is also a pervasive control and can be tested in a generic audit. An audit plan should, therefore, include a generic crown jewel audit for testing pervasive controls and other crown-jewel-specific audits.

Data Models and Automation

The smart auditor should use automation to reduce effort on certain audits, as the automation will perform continuous testing on the full population of items within the audit scope for the full period under review, reducing the need for sampling. Automation includes creating data models of audit items with attributes relating to key controls that must be tested, and it utilizes source data relevant to the attributes that update frequently, augmented by RPA.

Auditors can achieve a real-time view of the full population of items and obtain substantive evidence of key control performance by measuring the attributes in data models. Many controls from

the internal control environment can be mapped to attributes that form a part of the audit items (e.g., workstations, users, servers) by applying the principles described in the article on practical cyberrisk management.[9] The auditor can utilize existing models built by the business cyberteams or create new audit-specific models.

In the temperature monitoring system example discussed, a key control is the use of two-factor authentication by the users who log on to the system. If the users who use the system are identified as users of the temperature monitoring system crown jewel and are captured on a spreadsheet, the spreadsheet can be imported as a table in the data landing zone, and a temperature monitoring system crown-jewel-affected attribute can be added to the user model. The cyber management information system (MIS) can be programmed to extract data from the two-factor authentication system and the table imported and linked to the user model as well. The auditor can then create a metric in the MIS that informs him or her the moment a user working on the temperature monitoring system is no longer required to use two-factor authentication.

Similarly, if cyberawareness training campaigns and results are imported into the MIS and linked to the user model, the auditor will be able to monitor if crown-jewel-affected users are not performing their awareness training when modules are rolled out to users or if specific campaigns are not rolled out to crown-jewel-affected users.

The more automation that the auditor applies to testing of controls, the more resources will be available to perform audits on other crown jewels on the list and the more time will be available to identify new automation opportunities and improve existing automation. The smart auditor will use his or her expertise to develop automation of controls testing instead of performing manual or repetitive audit work.

Where the auditor is faced with legacy systems and it is difficult to extract data, or in environments where work is repetitive, RPA can be applied. RPA is the process of automating repetitive tasks by a robot that can be programmed to perform tasks that a human would normally do.

Using the temperature monitoring system example, one can assume it is a legacy system with little or no auditing and reporting functionality, and the database is proprietary and does not support modern database connections to extract data and utilizes local user accounts. A traditional audit approach could be for the auditor or another user to log on to the system with a special user account and extract information from various user accounts or system configurations that are required for testing, or to observe paper evidence of earlier extraction of data where the data were externalized and reviewed by management. In this case, RPA can be applied by programming a robot to log on to the system, read fields on the user screens, and write the relevant data to another system or even into a spreadsheet that can then be consumed by the MIS and linked to the relevant models. The robot can perform the task on frequent intervals and perform a full population test. The RPA process can inform the auditor when there are exceptions.

In general, controls should be implemented and performed by business management and output reviewed by the auditor. Control design should include the measurement of the control with an output that is relevant to the auditor, preferably in an automated fashion or in a format that is well suited for automation. A well-designed control includes not only the control itself, but also the measurement thereof and the use of the output for audit purposes.

> A WELL-DESIGNED CONTROL INCLUDES NOT ONLY THE CONTROL ITSELF, BUT ALSO THE MEASUREMENT THEREOF AND THE USE OF THE OUTPUT FOR AUDIT PURPOSES.

Conclusion

Cyberaudit planning and detailed assignment planning can be complex, and the risk exists that the plan does not address the real and relevant risk an organization faces. Executing on the plan can be tedious and manual in many cases. Applying crown jewel and attack path thinking, augmented by automation, can assist with creating a relevant audit plan and efficient use of scarce cyberaudit resources while executing the plan. The auditor should be familiar with the process to achieve this objective:

- Identify the crown jewels or utilize the crown jewel list created by the organization's management team.
- Perform threat modeling and attack-path mapping to understand how crown jewels can be attacked. If management has already done this, request the reports for analysis.
- Overlay attack paths on the Cyber Kill Chain, and identify key controls for each stage of the Cyber Kill Chain.
- Implement an MIS solution with data models and relevant attributes populated from data sources. If an MIS already exists, include the relevant attributes and data sources that can be used to measure key controls for audit purposes.
- Identify opportunities for automation and implement them through data modeling and RPA.

Author's Note

The views expressed in the article are those of the author and do not necessarily represent the views of his employer.

Endnotes

1 The Institute of Internal Auditors, *International Standards for the Professional Practice of Internal Auditing (Standards)*, USA, 2016, *https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf*

2 Deloitte, "CEO and Board Risk Management Survey: Illuminating a Path Forward on Strategic Risk," 2018, *https://www2.deloitte.com/us/en/pages/risk/articles/ceo-board-of-directors-risk-management-survey.html*

3 North Carolina State University's Enterprise Risk Management Initiative and Protiviti, *Executive Perspectives on Top Risks 2019*, USA, 2018, *https://www.protiviti.com/sites/default/files/united_states/insights/nc-state-protiviti-survey-top-risks-2019-executive-summary.pdf*

4 European Confederation of Institutes of Internal Auditing, *Risk in Focus 2019: Hot Topics for Internal Auditors*, 2018, *https://www.eciia.eu/wp-content/uploads/2019/02/Risk-in-Focus_2019.pdf*

5 Cloete, J.; "Practical Cyberrisk Management," *ISACA® Journal*, vol. 3, 2019, *https://www.isaca.org/archives*

6 Information Security Forum, *Protecting the Crown Jewels: How to Secure Mission-Critical Assets*, United Kingdom, *https://www.securityforum.org/tool/protecting-the-crown-jewels/*

7 Lockheed Martin, The Cyber Kill Chain, *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*

8 MITRE, "ATT&CK," *https://attack.mitre.org/*

9 *Op cit* Cloete