Teaching Case

Cybersecurity Assessment for a Manufacturing Company Using Risk Registers: A Teaching Case

Dr. Jim Marquardson
jimarqua@nmu.edu

Dr. Majid Asadi
masadi@nmu.edu

Northern Michigan University
Marquette, MI 49855, USA

Abstract

This case asks information systems analysts to assess the cybersecurity posture of a manufacturing company. The exercise works well as a group activity in an information systems course that addresses cybersecurity controls. The case introduces guidance from the National Institute of Standards and Technology, and learners develop work products consistent with the standards. The narrative provides high-level summaries of relevant cybersecurity standards. The case is based on a real company and actual projects, but the company name and specific details have been fictionalized and made more abstract to make this case relevant even when specific technologies evolve. Through this experience, students will learn the importance of a defense-in-depth strategy for securing information systems.

Keywords: cybersecurity controls, risk management, teaching case, manufacturing cybersecurity

1. INTRODUCTION

Organizations confront new cybersecurity risks every day in today's computerized world. They mitigate risks using a cybersecurity plan. Information systems professionals must understand cybersecurity concerns when designing and evaluating systems because the confidentiality, integrity, and availability of information systems must be protected. Malicious actors, whether inside or external to an organization, can try to steal company secrets, hold systems hostage for ransom, deface websites, corrupt data, try to crash systems, and more. No single process or technology can be implemented to protect information systems. Rather, multiple measures must be employed to protect systems with a defense-in-depth strategy.

In this teaching case, the cybersecurity posture of a manufacturing company is evaluated. The case is based on a real company and actual projects, but the company name and specific details have been fictionalized. The case introduces a risk register as a risk management tool for identifying and assessing potential cyber risks.

2. ABOUT ACME

ACME designs and manufactures tables and chairs for use at schools, weddings, conferences, and organizations that require easy setup and teardown of seating arrangements. The company invested significant money into research and design (R&D) to develop tables and chairs that are both sturdy and light. ACME can produce tables that weigh significantly less and are more durable than similarly sized particleboard-based tables by using a patented combination of wood,

metal, and plastic materials. The use of several materials also insulates them to some degree from fluctuations in the price of raw materials. ACME can charge a premium for its products with the promise that they will last for years.

ACME realizes that it must continue to innovate to stay relevant in the market. Patents on some of their existing products will expire shortly. Competitors are designing tables and chairs just different enough to avoid patent infringement. It has been increasingly difficult for ACME to charge a premium for its products. Company officers have decided to invest significant capital into designing a new table and chair. ACME would also like to expand its product line with lecterns. The new tables, lecterns, and chairs are codenamed the T1001, L1001, and C1001.

Embarking on the design of new products has caused ACME to reflect on its cybersecurity posture. If competitors were to infiltrate the company's systems and steal the R&D documents, ACME fears that the business could be ruined. ACME would like to conduct a full cybersecurity assessment. ACME would like its cybersecurity posture documented in a risk register. Risk registers and their components will be described in the following section.

3. CYBERSECURITY FRAMEWORKS

There are many cybersecurity frameworks that integrate industry standards and best practices to help organizations manage their cybersecurity risks (Taherdoost, 2022). While all these frameworks aim to protect data and contribute to a stronger security posture, they also have their own unique characteristics. Two popular frameworks are the Cyber Security Framework published by the National Institute of Standards and Technology (NIST) and ISO 27001 published by the International Organization for Standardization (ISO).

NIST created the Risk Management Framework and Cybersecurity Framework to help U.S. federal agencies and private organizations better manage cybersecurity risk. NIST's frameworks are open and readily accessible to the public. NIST documents often remind readers that the content is to be used to guide risk management processes rather than serve as a checklist of best practices. Therefore, organizations must think critically and use sound judgment when adopting NIST's guidance.

ISO 27001 is an internationally recognized standard that concentrates on security in information systems management (ISM). It is possible for organizations to become ISO 27001 certified through formal audits. Small- and medium-sized businesses and startups usually start their cybersecurity plans with NIST and work their way up to ISO 27001 as they scale (Alshboul & Streff, 2015).

ACME is a mid-size business based in the United States and would like to become a supplier to the United States Department of Defense. Department of Defense suppliers must comply with NIST standards. Therefore, the remainder of this case focuses on NIST documents and recommendations. The remainder of this section describes relevant NIST documents and how they can aid in the risk management process and development of risk registers. NIST makes these documents available without cost on its website, https://csrc.nist.gov/publications.

NISTIR 8286: Risk Registers

Column	Description
ID	A sequential number that identifies a specific risk
Priority	The relative criticality of the entry (e.g., low, medium, or high)
Risk Description	A brief overview of the risk, often stated in terms of cause and effect
Risk Category	A set of categories consistent with other risk registers in an organization
Likelihood	Probability of the event happening (1=low, 10=certain)
Impact	Consequences if the event happened (1=negligible, 10=catastrophic)
Exposure Rating	A multiplication of likelihood and impact
Risk Response Type	Approach to risk (i.e., accept, transfer, mitigate, avoid)
Controls	Technical, operational, managerial, or physical controls that mitigate threats

Table 1: Risk Register Columns

Organizations use risk registers to document threats, the likelihood of threats occurring, threat severity, and controls put in place to mitigate threats. NIST Interagency or Internal Report (NISTIR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* contains guidance on creating risk registers (Stine, Quinn, Witte, & Gardner., 2020). Table 1 summarizes

key risk register columns. An example table with sample records is included in Appendix A.

NIST 800-30: Threat Identification

NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, contains a taxonomy of threat sources and events (Joint Task Force Transformation Initiative, 2012). Appendices D and E in the NIST document list dozens of threat sources and sample threat events. Organizations can refer to NIST 800-30 to determine if they omitted relevant threats. Populate this information in the "Risk Description" column of the risk register. The list below summarizes threat sources and gives examples of each threat:

- Adversarial
  - Outside hacker (e.g., a hacker with no affiliation with the organization)
  - Trusted insider (e.g., a company executive)
  - Privileged insider (e.g., an authorized information technology administrator)
  - Competitor (e.g., another company)
  - Nation-state (e.g., state-sponsored hackers)
- Accidental
  - User (e.g., filing clerk)
  - Administrator (e.g., database administrator)
- Structural
  - Computer network outage (e.g., power supply failure)
  - Temperature controls failure (e.g., overheating in the data center)
  - Operating system failure (e.g., memory leak consuming all resources)
- Environmental
  - Natural disaster (e.g., flood)
  - Power outage (e.g., long-term outage due to major disaster)

The following are example threat events consistent with NIST 800-30 in Appendix E:

- Successful phishing attack: A competitor pretends to be a supplier and obtains detailed product specifications from the company.
- Successful denial of service attack: An adversary points a botnet at the company website to overwhelm the web server with requests.
- Earthquake at company headquarters: An earthquake disrupts power and network connectivity.

NIST 800-39: Risk Responses

NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* contains a "Responding to Risk" section that describes how risk can be accepted, avoided, mitigated, or transferred (Joint Task Force Transformation Initiative, 2011). These response types map to the "Risk Response Type" column in the risk register. Key risk responses are summarized below.

- Risk Acceptance: An organization chooses to engage in an activity if the risk is within its tolerance. For example, the risk of damage from a tornado can be low or high depending on a data center's geographic location. A company might accept the risk of tornado damage if it is in a tornado-prone area and the organization has a high risk appetite. An organization might accept the risk if the likelihood of a tornado is low and the organization has a low risk appetite.
- Risk Avoidance: An organization chooses not to engage in an activity because it is above its risk tolerance. For example, a company might decide not to co-locate its equipment in a shared data center because of privacy concerns.
- Risk Mitigation: Actions to reduce risks to an acceptable level. Common cybersecurity controls, like requiring multifactor authentication, can help to mitigate risks. Risk mitigation efforts are the most common entry on risk registers.
- Risk transfer: Organizations shift risk to another party. In cybersecurity, risk transfer is often implemented through buying cybersecurity insurance. An organization might implement security controls but still purchase cybersecurity insurance because the cost of a major data breach could be very high.

NIST 800-53: Controls

NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, details different controls that can be implemented to manage risk (Joint Task Force Interagency Working Group, 2020). This can be used to populate the "Risk Response Description" column of the risk register. Sample controls are listed below.

- All Wi-Fi access points require the use of a modern encryption protocol.
- Vulnerability scans will be run on all internal systems quarterly.
- All employees receive acceptable use policy training on an annual basis.
- A wireless guest network will be segmented from the employee network.
- An electronic badging system controls access to all buildings.

4. ACME'S CYBERSECURITY POSTURE

Security of the R&D process is of paramount importance to ACME. The product designs contain proprietary information that will be patented. Corporate competitors and suppliers should not have access to the design specifications until ACME files patents. The public should not see prototypes of the T1001, L1001, and C1001 until the models are ready for purchase. To protect the R&D process, ACME has instituted several safeguards. The company president and the Chief Information Security Officer (CISO) review these safeguards annually.

Campus Security

The ACME headquarters campus is open to the public. People can park in the company parking lot without passing through security. All guests must check in with the reception desk in the main building. Guests present photo identification and sign a log maintained by a security guard. Once guests are signed in, they must wear a sticker that identifies them as guests. Company employees escort visitors for the duration of their stay on the company campus. ACME issues smart cards with photo identification to all employees. Company policy dictates that employees present their smart cards whenever they are on campus. A central system controls access to buildings using smart cards and electronic locks.

The campus contains three buildings. The main building has areas for hosting guests, product demonstrations, and offices for office workers such as accountants, information technology staff, and company officers. The manufacturing building is the largest building on campus. It holds raw materials, finished goods, and the machinery required to build the products. The third building is the R&D building. Discussion of new designs, consumer research, prototype development, and testing is confined to the R&D building.

The R&D building has two entrances. The first entrance is a door for employees that automatically locks when closed. Employees must swipe a smart card on a smart card reader which grants them access. The door has a motion detector inside the building that automatically unlocks when an employee exits. The second door is a large roll-up door used for large materials and machinery. This door is locked from the inside with a padlock. Only two employees—the chief of R&D and the company president—have keys to the padlock. Bollards surround the R&D building. A water-based fire sprinkler system protects the R&D building from catastrophic fire damage.

Security cameras monitor the interior of the main campus building and the manufacturing building. No cameras are in use inside the R&D building. Security cameras also monitor the exterior of each building on campus. The camera data feeds are sent to the data center, to a server kept in a large utility closet in the main building. Policy prohibits the use of photographic equipment such as smartphones with built-in cameras in the R&D building.

Visitor Policies

ACME implements a strict visitor access policy since visitors can steal intellectual property, collect information, become injured in hazardous manufacturing areas, or threaten the safety of employees and other visitors. All suppliers, contractors, and delivery personnel are subject to this policy. Controls such as requiring an appointment, check-in, check-out, visitor badges, and guest internet network are part of this policy. No visitors are allowed into ACME's R&D building unless authorized by a department manager. This rule includes the company employees during off-duty hours too. The requests for permission to enter the building must be made at the front office. Personal visitors, including friends and family, are not permitted to access the building during or outside normal business hours. An appropriate associate must escort the visitor to the building.

Authentication and Authorization

Once a year, the company president reviews smart card access logs. The logs contain the employees' information and the location where access was attempted. The president manually scans the logs for access that might be unusual. The president also determines if access is appropriate for all employees based on their job duties. If a change to access levels is necessary, the president submits an access change request to the head of information technology operations who then makes the necessary change.

Technology for Research and Design

The engineers responsible for R&D do their work using Windows computers. The computers

connect to the internet to allow the employees to research existing patents, price materials, and conduct market research. The internet connection is separate from the internet connection used by the other buildings on campus. The network in the R&D building is segmented from the rest of ACME's network. The computers inside the R&D building can access the computing infrastructure inside the same building or the internet, but no other computer on ACME's campus. All computers' external USB ports are disabled unless authorized by a department manager. The computers employ screen-saver passwords and privacy filter screens.

The floor plan is very open and not conducive to having a dedicated telecommunications closet. The internet service provider's cable modem sits on a shelf in a corner of the R&D building. The cable modem is connected to a router that only has wired connections. The router connects to a unified threat management (UTM) device. The UTM device is then connected to an unmanaged switch. All workstations in the R&D building connect to the unmanaged switch. The workstations are manually configured with IP addresses to point to the UTM appliance for their default gateway. The UTM provides basic malware prevention, intrusion detection, and web filtering. Full disk encryption is enabled on all computers in the R&D building. Though most computers at ACME have users authenticate with a central Active Directory server, the strict network segmentation of the R&D building prevents those computers from accessing the central Active Directory infrastructure. Employees log in to the workstations in the R&D building with a local account using a username and password. The employees must update their passwords every three months.

All computers in the R&D building can access a central file server. The server allows anybody who knows the IP address to connect with full access to read and write files. Because physical access to the R&D lab is controlled, no authentication is required to access the file server. Employees use the file server to share files and collaborate. The file server is backed up using an external hard drive weekly, just like the workstations.

Employees make weekly full backups of blueprints, market research, and other files critical to the R&D process. Employees make backups by copying files to external hard drives. They store the external hard drives in a locked cabinet in the R&D building. Again, only the chief of R&D and the company president have keys to the cabinet. They maintain three weeks of backups.

R&D employees use computer-aided drafting tools, email, and basic office productivity software for the majority of their work. At times, they need the ability to install software, so they have been given administrative access to their computers. Like all ACME employees, R&D employees must still abide by the company's acceptable use policy, which states that they should not install software without proper licensing. Penalties for violating the acceptable use policy include censure and termination of employment. The R&D employees receive cybersecurity awareness training annually to prevent and mitigate cyber-attack risks.

5. STUDENT ASSIGNMENT INSTRUCTIONS

Assess ACME's cybersecurity posture by creating a risk register. Develop the risk register by evaluating cybersecurity threats and controls that could help mitigate those threats. Figure 1 shows the cybersecurity framework used at ACME for cyber risk assessment.

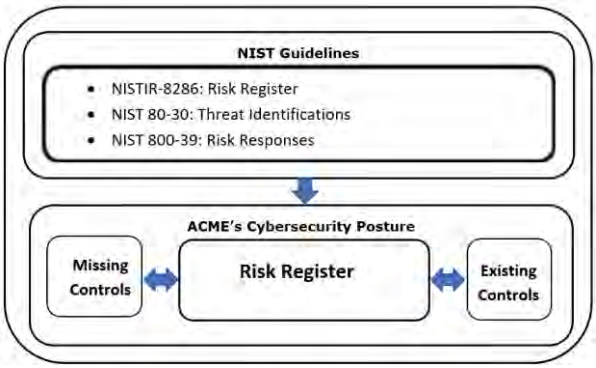

Figure 1: ACME's Risk Assessment Using a Risk Register

Professionals can employ a control-driven or event-driven approach to complete the risk register.

Control-driven Approach

In a control-driven approach, the existing controls are documented, then the adverse cybersecurity events that those controls mitigate are described. For example, a company might have fencing around its campus perimeter. Fencing is a known physical control, so it is clear that the company wants to keep people out. In the risk description column, document the specific reason why people need to be kept out. The control-driven approach largely focuses on what organizations are already doing.

Threat-driven Approach

Instead of focusing on controls already in place in the control-driven approach, the threat-driven approach emphasizes thinking about what could go wrong. Once the adverse events have been described, controls can be identified. For example, employees might be able to install software on their computers which could lead to them installing malware. A control could be restricting the ability to install software by non-administrative users. Gathering cybersecurity professionals with a variety of expertise together to brainstorm can help to find the essential controls and to identify the potential threats in the company. The threat-driven approach helps identify missing controls.

As company environments grow increasingly complex, professionals utilize proven methodologies capable of guiding a comprehensive, systematic assessment of cybersecurity threats. For example, some common methodologies such as OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation™) and TVA (Threat-Vulnerability-Asset) have been utilized to facilitate the identification of critical IT resources, the threats to those IT resources, and the identification of related system vulnerabilities (Mejias, Shepherd, Fronmueller, & Huff, 2019).

Risk Ratings

Once the risk description and controls have been documented, the remaining columns in the table can be completed.

1. For ID, enter a sequential number.
2. For priority, enter low, medium, or high based on your subjective assessment.
3. For risk category, choose confidentiality, integrity, or availability. Assume that ACME had formally adopted these categories.
4. For likelihood, choose a number from 1-10, 1 representing the lowest and 10 representing the highest likelihood.
5. For impact, choose a number from 1-10, 1 representing the most negligible impact, and 10 representing the most critical.
6. For exposure rating, multiply likelihood and impact.
7. For risk response type, determine if the risk response type is to accept, transfer, mitigate, or avoid.

Key Questions

It is important to be thorough on a risk register. Failure to identify relevant threats may lead organizations to develop insufficient controls. Failure to document existing controls might make some organizations believe that current practices are a waste of resources. Developers of risk registers should ask themselves the following three questions until they feel satisfied that no significant items are missing.

- What threats exist that have not yet been documented?
- What controls does the organization employ that have not yet been documented?
- What additional controls should we put in place to mitigate risk?

As a risk management tool, the risk register helps cybersecurity professionals and organization leaders agree on the proper approach to cybersecurity.

6. CONCLUSION

Cybersecurity is a process, not an end state. Part of that process requires professionals to evaluate threats and controls that mitigate those threats. This paper asks students to assess the cybersecurity posture of a manufacturing company via risk registers. Risk registers help organize and prioritize cybersecurity resources. As a communication tool, risk registers help information technology professionals and organization leaders reach a shared consensus on the role of cybersecurity in achieving organizational objectives. NIST provides detailed guidance on completing risk registers and other risk management processes.

7. REFERENCES

Alshboul, Y., & Streff, K. (2015). *Analyzing information security model for small-medium sized businesses.* AMCIS 2015 Proceedings.

Burke, A. (2011). *Group work: How to use groups effectively*. Journal of Effective Teaching, 11(2), 87-95.

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Joint Task Force Transformation Initiative. (2011). *Managing Information Security Risk: Organization, Mission, and Information*

System View (NIST SP 800-39; 0 ed., p. NIST SP 800-39). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Mejias, R. J., Shepherd, M. M., Fronmueller, M., & Huff, R. A. (2019). *Using Threat Vulnerability Asset (TVA) Methodology to Identify Cyber Threats and System Vulnerabilities: A Student Field Project Case Study.* Business Education Innovation Journal, 11(1).

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286

Taherdoost, H. (2022). *Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview.* Electronics, 11(14), 2181

Appendix A

Sample Risk Register Entries for Students

The following example show sample entries for a risk register. This can be provided to students in a template.

ID	Priority	Risk Description	Risk Category	Likelihood	Impact	Exposure Rating	Risk Response Type	Controls
1	Low	Employee leaks records to the media resulting in reputational harm	Confidentiality	2	4	8	Mitigate	All employees must sign a non-disclosure agreement that a lawyer has vetted
2	High	File server hard disk fails leading to data loss	Integrity	2	9	18	Mitigate	- Files will be backed up to the cloud nightly - Restoration from backup tested quarterly
3	Medium	Customer data breached by hackers leading to costs to contain the breach and legal fallout	Confidentiality	2	7	14	Transfer	- Cybersecurity insurance policy purchased - Data breach playbook created

Guide for Each Column
Assume that ACME has adopted the following standards for completing its risk register.

- ID: Sequential numbering
- Priority: Low, Medium, or High
- Risk Description: What can go wrong
- Risk Category: Confidentiality, Integrity, or Availability
- Likelihood: 1-10 (1=low, 10=high)
- Impact: 1-10 (1=10, 10=high)
- Exposure Rating: Likelihood multiplied by impact
- Risk Response Type: Mitigated, accepted, transferred, or avoided
- Controls: Technical, operational, managerial, or physical controls that mitigate the threat