Risk Assessment/Business Continuity

Assignment: Utility Providers

Created by Bobcat Consultation's Risk Management Team:

Amari (AJ) Jones

Maryrose Nguyen

Alaina Leary

Jason Jones

Isabella Ramirez

Table of Contents

Executive Summary

Our team recently took on the role of management consultants specializing in risk management and business continuity, and this project was our first big assignment. We were asked to work with a client to evaluate potential risks—especially those affecting IT systems—and to help build a strategy that would keep the business running smoothly during unexpected disruptions.

To start, we completed a Risk Assessment focused on three main threats: cyberattacks (like ransomware or phishing), equipment failures (such as server crashes), and natural disasters (for example, wildfires that could damage local data centers or knock out power). We looked into what security measures the company already had in place and offered new strategies to reduce risk—like investing in cloud backups, better firewalls, and routine cybersecurity training for staff.

Next, we moved into the Business Impact Analysis. This part helped us figure out which parts of the company absolutely need to stay up and running. Things like customer service systems, order processing tools, and access to employee data were top priorities. We considered how long each function could realistically be down without major financial or reputational damage. We also factored in how the industry's margins affect how long they can afford to pause operations—some businesses can weather a brief outage, but for others, even an hour of downtime is a big deal.

From there, we developed a Business Continuity Plan. This included:

- A clear Incident Response Plan that outlines what to do depending on the type of emergency,
- A Communication Plan so everyone—employees, customers, vendors—stays informed during a crisis,
- Steps for Backup and Recovery, with a focus on data protection,
- Ideas for Redundancy and Failover, like having mirrored systems or using cloud services to reduce downtime,
- And finally, a breakdown of Who's Responsible for making sure all of this gets done, plus how often the plan should be reviewed and updated.

Risk Assessment

Threat Assessment

There are many risks that may appear within a utility provider's company like *third-party/vendors, weak authentication or access control, denial-of-service attacks, unpatched or outdated systems, physical security breaches*, and much more. However, with this, we will follow up on three very likely and high-level risks.

1. **Ransomware**
    - Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting it with a group behind this encryption. That group will then demand a ransom for decryption. (NCSC)
2. **Nation-State APTs**
    - Advanced persistent threats (APT) actors are well-resourced and engaged in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion (CISA).
3. **Insider Threats**
    - An insider threat is a trusted individual who has been given access, or has knowledge of, any company resources, data, or system that's not generally available to the public (Microsoft).

Risk Analysis

1. **Ransomware**
    a. **Likelihood**: Common
    b. **Risk Level**: Very High
    c. **Impact on Business**: Ransomware attacks can cripple, or even cause catastrophic harm to company data and its operations, especially in organizations where the data is critical. It can cause damage to the reputation and also cause financial loss (Perception Point).

2. **Nation-State APTs**
    a. **Likelihood**: Medium
    b. **Risk Level**: High
    c. **Impact on Business**: Nation-State APT can cause major economic impact, reputational damage, and the supply chain management.
3. **Insider Threats**
    a. **Likelihood**: Medium-High
    b. **Risk Level**: High
    c. **Impact on Business**: The impact of an Insider Threat varies depending on how much the threat knows or has access to. It can vary from reputation damages to a total loss on the company.

Current Security Measures

- Incident Response Plans (IRP)
    - An IRP in place ensures utility providers can promptly identify, contain, respond to, and recover from security incidents while fulfilling reporting obligations.
        - *Standards to be in accordance with: NERC CIP & NIST SP 800-61*
- Firewalls and Network Segmentations
    - Perimeter defense via firewalls is required under *NERC CIP-005* to protect Electronic Security Perimeter (ESP) and restrict traffic between IT and OT systems, reducing attack surface.
- Endpoint Detection and Response (EDR)
    - EDR solutions provide real-time monitoring and automated response capabilities, helping detect and mitigate endpoint threats.
- Regular Software Patching and Updates
    - System patching should be a regular occurrence in order to mitigate known vulnerabilities. This process supports regulatory expectations around vulnerability management.
- Security Awareness Training for Staff

    - Training programs conducted should help meet and ensure personnel understanding of cybersecurity risks, and safe practices.
- Physical Security Control at Facilities
    - Physical protection measures, including surveillance and access controls ensure only authorized personnel have access to critical infrastructure and equipment.
- Compliance with Regulations and Standards
    - Governments and regulatory bodies worldwide have established cyber security standards for energy and utility sectors and businesses globally. Compliance with these is not only a legal requirement but also essential for maintaining operational integrity and customer trust.

Risk Mitigation Strategies

- Implementation of a Zero Trust Architecture
    - This will enhance security by reducing the attack surface, limiting lateral movement, and providing better threat visibility. (Szanowski)
- Regular Penetration Testing and Red Teaming
    - This will significantly enhance an organization's cyber security posture by proactively identifying vulnerabilities, improving incident responses, and ensuring regulatory compliance. (Harvey)
- Data Backup & Rapid Recovery Plans
    - This can minimize downtime, protect against cyber threats and enhance compliance. Additionally, this enhances customer trust and reduces costs. (Pollard)

Business Impact Analysis

Critical Functions

One of the most vital systems for a utility provider is the Supervisory Control and Data Acquisition (SCADA) system, which allows for remote control and real-time monitoring of assets such as substations, water flow valves, transformers, and pressure systems. Because this system is directly responsible for the stability and security of public services, any degradation—like through a ransomware attack—can result in loss of control with potentially catastrophic outcomes (Department of Homeland Security [DHS], 2021). Because the threat is shared and severe (as demonstrated through the risk register), SCADA systems are the most critical asset and need to be recovered in an instant in the event of failure.

Secondary priority is the Outage Management System (OMS), supporting instantaneous response coordination in the event of interrupted water or electricity services. It consolidates grid and customer alert reporting and supports dispatch units to react accordingly. Nation-state Advanced Persistent Threats (APT), being traditionally stealthy, tenacious, and capable of disabling service delivery in bulk, are an immediate threat to this function. As OMS is a link between detection and response, it must function even in the case of long-term cyber campaigns (North American Electric Reliability Corporation [NERC], 2022). The Customer Billing and CRM Systems facilitate customer communication, metering, invoicing, and compliance with data privacy. These systems are particularly at risk of insider threats, such as data leaks or malicious setups. While not potentially life-ending in the same way that a SCADA malfunction is, outages of these systems can result in revenue collection delays and erosion of customer trust. Access control assurance and auditing of user behavior are critical for risk mitigation (National Institute of Standards and Technology [NIST], 2020).

Network infrastructure and access control—VPN, firewalls, multi-factor authentication (MFA), and behavior analytics—is a universal dependency for every system. It is a building block in attack prevention and recovery. Because threats like ransomware and APT exploit vulnerabilities in access control and monitoring, this layer of security needs to be tested and updated regularly (Federal Energy Regulatory Commission [FERC], 2023).

Finally, the backup and recovery feature are the last line of defense, particularly in the case of ransomware where data can only be recovered through clean backups. Offline backups and rapid isolation of compromised systems are pointed out by the risk register. Without good backup and restoration capabilities, complete recovery from major threats would be extremely difficult or even impossible (IBM, 2023).

Downtime Tolerance

Downtime tolerance varies by function but is extremely low for most utility operations due to regulatory and public safety demands. SCADA systems are restricted to 15 minutes of acceptable downtime due to their real-time control role. OMS systems are able to withstand up to one hour, but after that, delays may affect emergency response and customer safety. CRM and billing systems can withstand one business day before there are financial and compliance issues. Network infrastructure must be restored within 30 minutes to prevent systemic failure, and backup systems must be up and running within 12 hours to enable recovery and prevent data loss.

These tolerances are not just on internal operational needs, but also on regulatory standards set by organizations such as NERC, FERC, and the Environmental Protection Agency (EPA). Failure to meet uptime levels can result in regulatory penalties, class-action lawsuits, and federal investigations in the event of compromised public health or critical services (EPA, 2022).

Financial & Operational Impact

Ransomware, as "very high risk" in the register, has the potential to result in loss of SCADA control, inducing shutdowns in water pumping stations or power substations. It not only impacts public services but also imposes tremendous recovery costs, including emergency IT personnel mobilization, legal consultation, public relations, and ransom payment in certain instances. Secondary costs include long-term loss of public trust and increased regulator attention (IBM, 2023).

Nation-State APTs pose a more menacing and strategic threat and can potentially create major outages and data exfiltration. APTs are difficult to detect and often use anomaly detection mechanisms, which many aging systems lack. Effective APTs can knock out large segments of the grid or water infrastructure and exfiltrate sensitive data, leading to long-term operational degradation and geopolitical consequences if blamed on foreign influence (NERC, 2022; DHS, 2021). Insider threats, though too often underestimated, are also very damaging. Privileged staff can silence alarms, remap SCADA protocols, or steal sensitive customer and operational data. The register classifies this as "high risk" with medium-high likelihood, and to manage it one requires both behavior analytics and stringent access control policy. Financial loss can involve in-house investigations, data mishandling penalties, and trust remediation between customers and staff (NIST, 2020).

Business Continuity Plan

Incident Response Plan

The purpose of this Incident Response plan outlines the procedures, roles, and priorities for detecting, containing, eradicating, and recovering from cybersecurity incidents that may affect the Utility providers' IT systems and data. The goal of this plan is to help minimize the disruption of business operations, protect critical functions, ensure the safety of the utility services and public, as well as comply with regulatory requirements. (Public Power, 2019)

The scope of this plan applies to all Utility employees, contractors, and third parties using the utility's IT assets including the networks, systems, applications, or data. This plan will apply to all cyber incidents.

Cyber Incident Response Team

Incident Response Manager

Operations Lead

Legal Counsel

Public Affairs/Communications

NERC CIP Manager

*Responsibilities are defined below in the communication and execution plans

Phase one: Preparation

- Regular training and simulation exercises will be conducted to ensure the IRT and relevant staff are familiar with their roles and responsibilities
- Necessary tools like forensic software and communication platforms will be maintained and readily available

Phase two: Detection

- Track and assess threat and vulnerability information
- Report cyber threats and suspicious activity alerts to the cyber incident manager
- Declare and classify a cyber incident
- Alert and activate the cyber incident response team

Phase three: Containment

- Identify initial actions to prevent further damage
- Document the incident from start to finish using approved handling forms in consultation with legal
- Follow procedures for forensic investigation, system imaging, and evidence gathering
- Conduct mandated reporting and notification within required thresholds and timelines

Phase four: Eradication

- Assess resource needs and available expertise to remove the threat
- Develop response procedures and assign responsibility
- Engage industry response partners to validate the incident and support mitigation when needed

Phase five: Recovery

- Restore the system to full operation by thoroughly testing all systems and applications to ensure functionality and data integrity
- Verify that mitigations were effective and the threat is removed
- Identify needed improvements to plans, procedures, and resources
- Conduct post-incident review meetings
- Update the plan with lessons learn

Communication Plan

Communication Plan Effective communication during an incident is critical for maintaining trust and ensuring coordinated recovery efforts (CISA, 2021).

- Communication Plan outlines:

- Internal Communications: IT and Security teams alert department heads and executives via secure messaging.
- External Communications: Customers and regulators are notified via pre-approved channels (email, press releases, public service announcements).

  Roles & Responsibilities:

  - Public Affairs/Communications handles messaging to employees, media, and customers.
  - Legal Counsel ensures all messaging complies with breach notification laws and regulatory expectations.
  - NERC CIP Manager coordinates with regulatory bodies to ensure compliance with incident reporting standards.

- Message Templates: Pre-written messages for different scenarios (data breach, service outage).

Backup & Disaster Recovery

Backup & Disaster Recovery plans ensure business continuity even in the event of total data loss or infrastructure compromise:

- Daily incremental and weekly full backups are stored both on-site and in the cloud.
- Offline backups are maintained monthly to prevent ransomware encryption (IBM, 2023).
- Recovery Time Objective (RTO): <12 hours for critical systems.
- Regular testing of recovery procedures every quarter (NIST, 2020).
- Secure access to backup environments to prevent unauthorized restore operations.

Redundance and Failover Strategies

Redundance and Failover Strategies are implemented to ensure high availability:

- Mirrored servers across geographically separate data centers (AWS, 2022).
- Load balancers to reroute traffic during peak load or failure.
- Real-time data replication for SCADA and OMS systems.
- Redundant power supplies and internet service providers.
- Automatic failover protocols tested monthly (NERC, 2022).

Plan Execution

- **Incident Response Manager:** Has overall authority and responsibility for managing the incident response process.
- **Operations Lead:** Represents operational technologies and ensures coordination and understanding of potential impacts on critical infrastructure.
- **Legal Counsel:** Provides legal advice and guidance on breach notifications and potential legal ramifications.
- **Public Affairs/Communications:** Responsible for internal and external communication regarding the incident, in coordination with legal counsel and the NERC CIP manager. Ensures consistent and accurate messaging to stakeholders and quickly responds to employee, media, and customer inquiries.
- **NERC CIP Manager:** Ensures that incident response actions and reporting comply with NERC CIP requirements.

Plan Maintenance

- Reviewed twice a year by the Cyber Incident Response Team (CIRT).
- Post-incident reviews are conducted for lessons learned and improvements.
- Annual drills test readiness and compliance.
- Stored securely and accessible to all team leads.

Conclusion & Recommendations

What did we learn about the industry

While researching the utility industry for the risk assessment we learned about the critical infrastructure. Utility providers operate critical infrastructure, like the SCADA system, that directly impacts the public's safety and well-being. Disruptions in these systems can have major consequences which emphasizes our need for security. We found the low downtime tolerance of the SCADA and OMS systems interesting as these systems have extremely low tolerance. Recovery time objectives must be aggressive to minimize the disruption to operations and public safety.

What do we recommend

Bobcat Consolations recommends implementing Zero Trust Architecture. This security feature removes the concept of implied trust, requiring strict verification for every user and device accessing the network. With this architecture threat visibility is improved and lateral movement of threats is limited. We also recommend regular penetration testing as this will help improve incident response capabilities and ensure compliance with regulatory requirements. Our final recommendation is to conduct security awareness training for staff. Awareness training will promote safe practices and educate employees about cybersecurity threats.

How feasible are our recommendations

We believe that the recommendations we provided are feasible for the average utility provider company as our plan is cost-effective and scalable. While some of our recommendations involve initial investment, they offer long-term financial benefits. For example, investing in recovery systems can prevent significant financial loss associated with data loss and downtime. Security awareness training can help reduce the likelihood of phishing attacks. As in terms of scalability, our recommendations of the Zero Trust Architecture are designed to be scalable. Which means they can be adapted to fit any small local operation or to a larger regional company.

Resources

"A Guide to Ransomware." *NCSC*, www.ncsc.gov.uk/ransomware/home.

Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA. www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors#:~:text=APT%20actors%20are%20well-resourced,network%2Fsystem%20disruption%20or%20destruction.

What Is Insider Threat? Unraveling Insider Risks | Microsoft Security. www.microsoft.com/en-us/security/business/security-101/what-is-insider-threat?ef_id=_k_CjwKCAjwk43ABhBIEiwAvvMEB-j3xDamAEBxI9-nKWVZ5i-0HaUq3I6N-RUb0IFSL8FFp-kbMEtgsxoCiZEQAvD_BwE_k_&OCID=AIDcmmdamuj0pc_SEM__k_CjwKCAjwk43ABhBIEiwAvvMEB-j3xDamAEBxI9-nKWVZ5i-0HaUq3I6N-RUb0IFSL8FFp-kbMEtgsxoCiZEQAvD_BwE_k_&gad_source=1&gclid=CjwKCAjwk43ABhBIEiwAvvMEB-j3xDamAEBxI9-nKWVZ5i-0HaUq3I6N-RUb0IFSL8FFp-kbMEtgsxoCiZEQAvD_BwE.

"How Ransomware Attacks Work: Impact, Examples, and Response." *Perception Point*, 25 Sept. 2024, perception-point.io/guides/ransomware/how-to-prevent-ransomware-attacks.

Szanowski, Przemyslaw. "What Is a Zero Trust Architecture and How Does It Work?" *Object First*, objectfirst.com/guides/data-security/zero-trust-security-architecture.

Harvey, Sarah. "5 Benefits of Penetration Testing on a Regular Basis | KirkpatrickPrice." *KirkpatrickPrice*, 22 June 2023, kirkpatrickprice.com/blog/5-benefits-regular-penetration-tests.

Pollard, Barry. "Top 6 Advantages of Data Backup and Recovery." *Adivi Corporation*, 15 Dec. 2023, adivi.com/blog/advantages-of-data-backup-and-recovery.

Department of Homeland Security. (2021). *Cybersecurity & Infrastructure Security Agency (CISA) – Industrial Control Systems Security*. https://www.cisa.gov/ics

Environmental Protection Agency. (2022). *Cybersecurity for the Water Sector*. https://www.epa.gov/waterutilityresponse

Federal Energy Regulatory Commission. (2023). *Cybersecurity Guidance for Utilities*. https://www.ferc.gov

IBM. (2023). *Cost of a Data Breach Report*. https://www.ibm.com/reports/data-breach

National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems*. https://csrc.nist.gov/publications

North American Electric Reliability Corporation. (2022). *Critical Infrastructure Protection (CIP) Standards*. https://www.nerc.com

Public Power Cyber Incident Response Playbook. publicpower.org. (2019, August). https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

NCSC (n.d.). A Guide to Ransomware
https://www.ncsc.gov.uk/ransomware/home

Microsoft (n.d.). What Is Insider Threat?
https://www.microsoft.com/en-us/security/business/security-101/what-is-insider-threat

Perception Point (2024). How Ransomware Attacks Work
https://perception-point.io/guides/ransomware/how-to-prevent-ransomware-attacks

Object First / Szanowski (n.d.). What Is a Zero Trust Architecture
https://objectfirst.com/guides/data-security/zero-trust-security-architecture

KirkpatrickPrice / Harvey (2023). 5 Benefits of Penetration Testing
https://kirkpatrickprice.com/blog/5-benefits-regular-penetration-tests

Adivi / Pollard (2023). Top 6 Advantages of Data Backup and Recovery
https://adivi.com/blog/advantages-of-data-backup-and-recovery