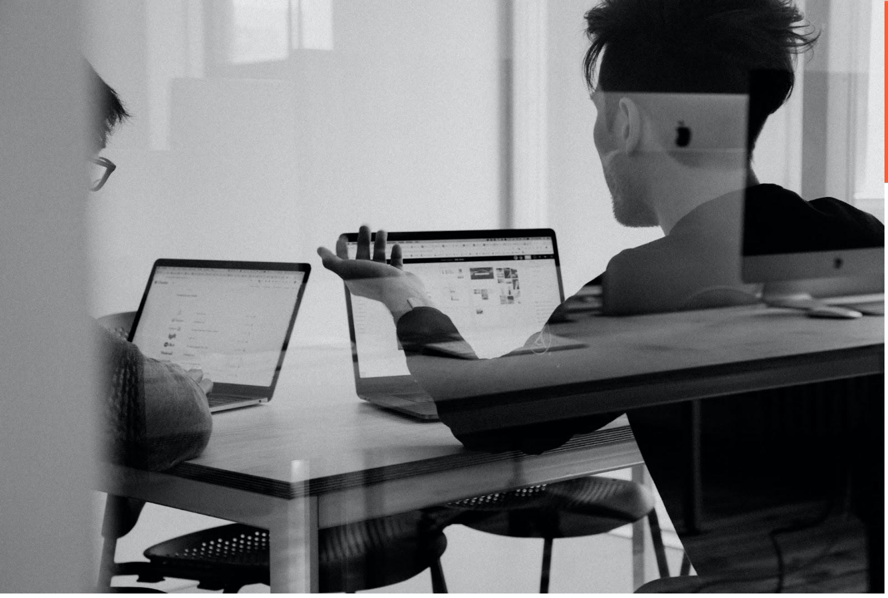
UKRAINE CYBER-INDUCED POWER OUTAGE: KRI Report

By:

Brandon Sigua	214933873
David He	211514890
Eric Traccitto	218835074
Harman Sandhu	215629967
Mohammad Fahim	219263094



ABOUT THE INCIDENT

On December 23, 2015, a cyber-induced power outage took place in three provinces in Ukraine affecting a total of 225,000 customers for a total of six hours (Owens 2016). This incident highlighted the threats to many control systems and outdated infrastructures worldwide, emphasizing the importance for organizations to review and strengthen their control systems. If the Ukraine Power Grid had proactively followed a key set of Key Risk Indicators (KRI) they could have been able to effectively manage and mitigate the impact of risk to the organization.

Methodology:

When developing our set of Key Risk Indicators (KRIs), we focused on the core business purpose that underlies KRIs. Specifically, KRIs serve the crucial function of pinpointing and overseeing the most significant risks that can potentially impact the achievements of the organization's business objectives. Consequently, our approach involved identifying the primary risks facing the Ukraine Power grid. In this approach, we realized that the areas posing the highest risk were linked to the assets with the greatest value. Once we had identified the most important assets, developing the KRIs for these assets entailed a threat modeling process for each asset. In this context, we kept in mind that assets with limited vulnerabilities are assets with marginal risk.

Key Considerations:

In addition to KRIs addressing the organization's most significant risks, we considered additional factors. It was important that the data for KRI's be easily, rapidly, and cost-effectively collected. Moreover, the KRI itself needed to be quantifiable and comparable in order to effectively gauge the efficiency of existing controls and the current residual risk. Distinguishing between various types of KRIs, such as leading, current, and lagging was our primary focus. We aimed for predictive, leading indicators, enabling the organization to proactively implement remedial actions and prevent cyber incidents before they occurred. However, the main concern in our KRI Design was ensuring that the metric precisely reflected the level of risk exposure, even if opting for a more costly or lagging indicator became necessary.

> It takes 20 years to build a reputation and few minutes of cyber incidents to ruin it. Technology trust is a good thing, but control is a better one. - Stephane Nappo

KRI 1: Secure Sign-On

Parameter:	Percentage of enterprise members logging in with Single Factor Authentication.
Risk Description:	The potential risk of unauthorized access by threat actors is being measured. The more users log in without a safe authentication method like MFA, the more likely it is for the threat actors to be able to get in using stolen information
Measurement of Risk Driver:	- High: 20% Single Factor Authentication - Medium: 10% Single Factor Authentication - Low: 2% Single Factor Authentication
Data Collection:	**Source:** The number of successful login attempts on the system recorded in a month that's done is separated to those done with single factor and multifactor authentication
Rationale:	After Gaining access to the Oblenergo's Microsoft Directory servers that contained the credentials of users, the threat actors proceeded to get into the Oblenergo network with ease. This happened because a control that is so simple to implement like multi-factor authentication wasn't in use. If it was in use, then the hackers couldn't get into the systems with credentials alone, which would make their work far more difficult
Action Plan:	If a very high percentage of the enterprise members are logging in without multifactor authentication, access to their accounts would get locked off until they'd set up multi-factor authentication.

KRI 2: Email & Web Security Software

Parameter:	Phishing Email Detection & Clickthrough Prevention.
Risk Description:	Employees may be unable to detect phishing emails from real corporate emails which can become problematic during a cyber-related attack. The first step in the Ukraine Power Grid attack in 2015 was using a phishing email to gain access to the Oblegenero network through workstations.
Measurement of Risk	- High: Detection of a large number of phishing emails with attributes closely matching known attack patterns.

Driver:	- Medium: Phishing emails indicating potential threats that require further investigation and response. - Low: Minimal or no detection of phishing emails present, suggesting a low risk of successful phishing attacks
Data Collection:	**Source:** Monitoring these trends over time can show patterns between phishing attacks. - User-reported incidents: Administrative review. - Email Filter System: Real-time continuous monitoring.
Rationale:	The very first step of the Ukraine attack in 2015 involved an email spear phishing attack that contained a Microsoft document that had a macro called black energy 3 which automatically installed itself onto corporate workstations (Owens 2016). Being at the very source of the beginning of such a large-stage attack, finding out how to detect and prevent the attack from carrying through the first stage is to take some technical measurements. Evidently, phishing emails are received by everyone, however, the Ukraine attack was viciously planned and studied by controlled individuals. If the enterprise network is able to measure the amount of phishing emails per month with the use of developing a Web Security Software compared to without this software, an enterprise network may prevent an email spear phishing attack or the link from activation which could prevent a macro such as BE3 from infecting workstations. These email security controls can truly benefit an enterprise network and aid in its success against successful blocking of malicious attempts at gaining access to the host's target networks. One study found the need for developing an algorithm to identify spam and malicious accounts on Online Social Networks was integral. Since 2011, approximately 65% of Americans have used an OSN (Wilson 2012). The study aimed towards fighting these spam and malicious accounts which were the primary tools at the given timeframe that hackers would sue as threats on the web (Wilson 2012). A second study revealed the "potentially high impact of the inclusion of email headers on the predictive accuracy of machines learning algorithms and the significance of enabling cost-sensitive measures as part of the learning process" (Tout 2013). The research was conducted in the study of machine learning algorithms that prevent phishing attacks through the accuracy of viewing email headers. The study concluded that it would be indeed more expensive to implement the machine learning technique that could also view the email headers properly themselves and decide whether the email was one of priority or one of a phishing attack. However, the study also concluded that

	implementing this extra step to the algorithm would indeed result in way fewer false positives and slightly more frequent false negatives.
Action Plan:	Both studies aim to the research of preventing phishing attacks to a higher degree, rather than having no machine learning technique or web-based software to prevent these vicious, hidden-email attacks on a company's hardware and workstations, such as the Oblenergo recipients who were phished with what they thought were official documentation from the Ukraine Energy Ministry (Owens 2016).

KRI 3: Failed Login Attempts	
Parameter:	Number of failed logins on an account.
Risk Description:	Counting the number of failed logins made on a single account helps to prevent attempts at brute forcing a password, which is to crack a password with trial and error.
Measurement of Risk Driver:	- High: 8+ attempts require immediate investigation. - Medium: 4 to 8 attempts should be monitored for actions. - Low: 1 to 4 attempts relatively low risk.
Data Collection:	The application keeps count of the failed login attempts
Rationale:	The active directory server at Prykarpattiaoblenergo was compromised using a brute force method in order to gain access to the credentials of the users. Proper defenses against brute force would’ve prevented the threat actors from gaining access to the user’s credentials.
Action Plan:	When the number of failed attempts against a single account reaches 8, that account is locked off, and a message about the event including the IP that tried accessing the account is sent to the account owner to know about the attempt against their account and also the data administrator so the proper measures can be taken against the possible threat actor.

KRI 4: Unusual Traffic Patterns

Parameter:	Detection of Unusual Traffic Patterns in organizations network.
Risk Description:	Patterns that may be flagged autonomously or by network administrators as suspicious due to abnormal behaviors in high-risk or critical infrastructure. This may indicate malicious activities such as reconnaissance or insider threats for possible DDoS attacks or unauthorized access attempts.
Measurement of Risk Driver:	- High: Unusual patterns consistent with known attack signatures. Change in user pattern from baseline: 40-100% - Medium: Unusual patterns that require further investigation. Change in user pattern from baseline: 20%-40% - Low: Normal traffic patterns. Change in user pattern from baseline: 5%-20%
Data Collection:	**Sources:** - Intrusion Detection Systems: Real-time continuous monitoring. - Firewalls: Real-time continuous monitoring. - Networking Monitoring Tools (behavior analytics): Regular intervals with periodic deep dives. - Network Logs (baseline traffic patterns): Periodic reviews and scheduled assessments.
Rationale:	In the case of the Ukraine Power Grid Incident, two key areas that should be addressed are the need for comparison tools and the limitations of controls. The absence of comparison tools for UTP, such as baseline, logging, and monitoring allowed the threat actors to move over the network undetected. This absence becomes a vulnerability that threat actors exploit to perform reconnaissance and enumeration of the network and establish a backdoor through an encrypted tunnel (Owens 2016). The lack of preventative controls is evident, as there were no measures to prevent the modification of access to other HMI admins or prevent them from hopping onto other segmented networks thus allowing the manipulation of breakers through remote access. As a result, they were able to harvest the credentials of workstations and HMI administrators, in order to lock out other HMI administrators. This was because they had gained access to the control center supervisory control and data acquisition HMI servers as they were not segmented properly (Owen 2016).

	Employing tools like network monitoring, user least privilege, Intrusion Detection Systems, and proper firewall configuration could have been instrumental in identifying abnormal events.
Action Plan:	When the risk level for UTP approaches or exceeds the high threshold, it is important to immediately isolate the affected systems from the network. This will help prevent unauthorized access in order to minimize the impact on critical systems and limit potential threats. It is also essential to coordinate the team's efforts throughout any investigation by following an incident response plan that outlines a coordinated strategy to identify, measure, respond, and continuously monitor potentially hostile traffic patterns. Using this proactive response to UTP will allow Ukraine's power grid to flag unknown traffic patterns for investigation and block known traffic patterns in order to perform any remediations that are required.

KRI 5: Optimum Patch Level Compliance

Parameter:	Identifying & Maintaining Optimum Patch Level (OPL)
Risk Description:	Inadequate compliance with recommended patch levels presents a considerable cybersecurity risk, exposing systems to vulnerabilities and elevating the risk of security breaches, data compromises, and operational disruptions. Ensuring optimum patch-level compliance requires promptly applying and maintaining the latest updates for software, operating systems, and applications. Neglecting these recommended patching practices results in exploitable weaknesses that malicious actors may take advantage of.
Measurement of Risk Driver:	- High: The OPL index falls below 80%, indicating significant vulnerabilities. - Medium: The OPL index is between 80% to 90% signifies moderate compliance to patch levels. - Low: The OPL index of 90% and above reflects strong compliance with optimum patch levels.
Data Collection:	**Sources:** - Automated scanning tools for system patch levels: Weekly - Monthly.
Rationale:	In the case of the Ukraine Power Grid Incident, it was quite evident that the use of anti-malware and network segmentation could have prevented the spread of this attack.

	The use of advanced whitelist anti-malware solutions, including endpoint protections and intrusion detection systems would have ensured to block all unknown and undesired applications from executing, including malware such as Black Energy 3 (BE3) (Owen 2016). However, due to the lack of up-to-date patching practices BE3 was able to infiltrate the enterprise systems and dedicated control systems through social engineering. Additionally, the lack of network segmentation made it easy access to the control server, as these servers were connected to the internet rather than placed behind configured firewalls that would have isolated them from the business network (Owen 2016). Effective network segmentation could have restricted the attacker's ability to move from compromised systems to critical systems. Prompt deployment of security patches through the use of proper anti-malware and network segmentation could have reduced the risk of cyber incidents tremendously. Additionally, OPL is essential to maintain system stability, prevent operational disruptions, and uphold organizational reputation.
Action Plan:	When the risk level for the optimum patch level approaches or exceeds the high threshold, this indicates notable vulnerabilities and an immediate patch is required. When evaluating what patch should be made, it is important to perform a comprehensive evaluation and ensure improvements are made to the patch management process. This raises awareness of possible risks that employees may be able to avoid and guarantees the deployment of critical patches before they pose a threat to the organization. Many businesses, including the banking and energy sector, have adopted this proactive approach, demonstrating the value of prompt decision-making and targeted action to fortify cybersecurity against ever-evolving threats.

KRI 6: Non-inventoried Application

Parameter:	The number of applications on the organization's system that are not accounted for in the official inventory.
Risk Description:	Application inventory helps organizations track and monitor applications within their organization. When undocumented

	applications are identified in an organization's systems they have to be investigated because it increases the potential risk of malware attacks and infiltration through these untracked applications. By effectively managing and responding to non-inventoried applications through the use of detection systems, organizations can mitigate the potential risk to an organization's infrastructure and servers.
Measurement of Risk Driver:	- High: Non-inventoried applications exceeding 5% of total inventory. - Medium: Non-inventoried applications between 1%-5%. - Low: Non-inventoried applications between 0%-1%.
Data Collection:	**Sources:** - System scans: Weekly scan. - Endpoint protection solutions: Real-time continuous monitoring - Network Monitoring tools: Real-time continuous monitoring
Rationale:	In the case of the Ukraine Power Grid Incident, it was quite evident that application inventory was not actively logged or monitored. This is evident as malicious actors were able to install malware, and software, and build backdoors on compromised computers without detection (Owen 2016). A way this could have been prevented was to provide all users with the least permission including HMI operators from installing/modifying applications on the server without the action scheduled in their logs. This could have given them an early indication that the team was able to pick up on these new applications and identify that they were not a part of the intended or future system updates. On the other hand, if a detection system was considered they would have been able to set alarms when the normal operation of control systems deviated beyond the preprogrammed and acceptable bounds (Owen 2016). These acceptable bounds could have considered unauthorized breaker actions, password changes, unusual network movement through undocumented applications, and other critical events. Addressing these non-inventoried applications is a proactive initiative required by the team as a whole to leverage their tools and knowledge to recognize possible threats. This will ensure the team safeguards the organization from potential security breaches, data compromise, and infiltration through undocumented channels.

Action Plan:	When the risk level for the non-inventoried applications approaches or exceeds the high threshold, the organizations need to conduct a thorough analysis of the non-inventoried applications to determine the nature and origin of these applications. If this application is marked as hostile it requires the immediate isolation of affected systems and removal/securing of the undocumented application. If the application is marked as inventory intended for the organization, an updated official inventory has to be performed.

KRI 7: Employee Education

Parameter:	**Completion of Employee Education & System Compromise Prevention**
Risk Description:	Employees click phishing emails that may potentially contain harmful malware. This can lead to a Systems Compromise Breach. During the Ukraine Power Grid Attack in 2015, Black Energy 3, a malicious virus implemented as a macro was installed on corporate hardware during the opening of a phishing email that contained a Microsoft document.
Measurement of Risk Driver:	- High: Low level of awareness & resulting in frequent security incidents. Below 50% - Medium: Moderate level of awareness & partial completion of cybersecurity-related courses that may indicate areas of improvement in employee education. 50%-79% - Low: High level of awareness & completion of cybersecurity-related courses that translate to low incidents. - 80%+
Data Collection:	**Source:** - Employee Training Records: Quarterly assessments. - Incident reports: Real-time reports. - Simulation of phishing exercise: Periodic phishing exercises.
Rationale:	There had been zero information regarding the Oblenergo staff being prepared for any technological attack or being aware of any threat that would shut down their power grids. A control that can help prevent this attack is user awareness. If staff have been made aware of simple yet powerful controls, in this scenario it would be double checking before opening documents from an email to make sure the email is sent from an actor inside the company and it is not a phishing attack, it can seriously avoid a huge catastrophe similarly to the 2015 Ukraine power grid attack. By measuring the percentage of phishing

	emails received and opened by recipients, and comparing that to the percentage of attendees who actually attended mandatory training for systems compromise prevention meetings, it would be evident that there would be a concrete difference. One study relieved the risk of how information becomes compromised and the appropriate ways to prevent such an occurrence from happening. One of the many sample suggestions related to prevention is stopping the source at its roots, aiming toward making sure all staff are aware and vigilant of situations that can emerge during any given time. “Developing a security awareness plan to make all employees Data Information experts, and to make employees at all levels aware of the value of corporate information and the importance of information management” (Helms 2000). Knowing how important it is to be aware of both surroundings and company policy can aid in the protection from outsider infiltration. The author has a large experience with learning about companies and their information technology countermeasures against disasters. A second study is a response to casualties resulting from poor risk management and human error. The author, René Amalberti, specializes in all types of safety related to disasters caused by risks regarding information compromises. The significance of disasters and attacks due to compromises in systems is quite large, and the reading provides some examples: “explosion at the Total AZF plant at Toulouse in 2001, the explosion at the BP oil refinery in Texas in 2005, the explosion at the Buncefield oil terminal in 2005, and the renewed European debt crisis in 2011 (involving the disappearance of perhaps USD 25 trillion)” (Amalberti 2013). The main purpose of the study is to conclude that human error plays a major part in defending the company's hardware or software in every scenario. An important rule created in the reading is how few employees understand that their job can be considered as important as the authorities in some cases when aspects of their job require a “safety model” in place by the company to guard information and data in the domain of the company.
Action Plan:	Considering if the data collection methods prove high, and using the references as proof, it will make sure that staff become educated in the workplace about the rules between network safety and system disaster prevention. Aiming for more communication, meetings, legal documents, and proper consequences of endangering others' lives to avoid cyber disasters similar to the 2015 Ukraine Power Grid Attack.

KRI 8: Insider Threat

Parameter:	Percentage of individuals with undefined/inappropriate duties or access levels.
Risk Description:	The risk here is associated with insufficient separation of duties, which is required to mitigate the threat posed by malicious or compromised individuals from within the organization. For example, if there is insufficient separation of duties, then there may exist high-risk individuals who may represent single points of failure. Additionally, damage from compromised accounts may be excessive if the accounts have more access than they should.
Measurement of Risk Driver:	● High: over 20% undefined/inappropriate duties/authorization ● Medium: 10-20% undefined/inappropriate duties/authorization ● Low: under 10% undefined/inappropriate duties/authorization
Data Collection:	Review of Segregation of Duties (SoD) Matrix, note conflicts and cross-reference against employee authorizations to note inappropriate access levels. Can be conducted on a monthly basis.
Rationale:	In the Ukraine attack, compromised corporate accounts had access to the SCADA network, due to improper router configuration. This allowed hackers to compromise the actual power plant systems associated with the SCADA system. The failure to limit the damage was due to improper access levels for the employee accounts, even though they had no theoretical access to the SCADA network.
Action Plan:	In the event that improper separation of duties or inappropriate authorization reaches unacceptable levels, remedial action should commence, beginning with a review of the SoD matrix to rectify designated assignment of duties. In the case that the organizational structure has been designed correctly, authorization levels should be adjusted to reflect the intended responsibilities, as according to the principles of need-to-know and least-privilege.

KRI 9: Data Recovery

Parameter:	Maintaining backup level resilience & frequent testing of backup processes.

Risk Description:	Measures the backup system's reliability and operational efficacy in protecting data integrity. When backup levels fall below the minimum acceptable time frames, it causes delayed recovery efforts and hinders the restoration of critical systems, data, and services. Because of the increased risk, it is critical to keep up a strong disaster recovery backup system in order to mitigate potential impacts on organizational resilience and operational stability.
Measurement of Risk Driver:	**Source:** The backup level falls below the minimum acceptable time frames: - High: The backup failure rate exceeds 10%. - Medium: The backup level failure rate is between 5% and 10%. - Low: The backup level failure rate is below 5%.
Data Collection:	Sources: - Failure Reports: Real-time continuous monitoring. - Backup System Logs: Periodic reviews and scheduled assessments. - Periodic Performance Reviews: Quarterly assessments.
Rationale:	In the case of the Ukraine Power Grid Incident, rewritten firmware, Telephony Denial of Service (TDOS), and KillDisk activation were three key events that played a huge role in the delay in recovering their systems. First, the attackers were able to overwrite firmware on substations through serial to ethernet converters rendering them inoperable and unrecoverable (Zetter 2016). This essentially left them with only one option, which was taking the system offline in order to completely replace these devices and in order to re-integrate them with the network manually. Secondly, they were able to minimize communications between the teams through TDOS which disrupted restoration efforts. As call centers were overwhelmed with automated calls from foreign numbers they were unable to document what technical failures were occurring with their systems (Owens 2016). Thus limiting the situational awareness they had on the severity of the attack, and what locations it was actively affecting. Thirdly, when they deployed malware called KillDisk, they wiped files from operator stations making them inoperable as they overwrote the essential system files, including the master boot (Zetter 2016). Hence, rendering many workstations inoperable, and having to be replaced in order to regain sufficient control of the network.

	Together, these events significantly contributed to the delay and complexity in recovering the power grid's systems, with many workstation documents lost permanently as they were deemed irrecoverable. Thus emphasizing the importance of maintaining optimal backup levels for operational resilience.
Action Plan:	When the risk level for backup-level resilience approaches or exceeds the high threshold, the activation of a comprehensive backup, and recovery system for critical workstations is essential. Simultaneously, the implementation of redundancy measures should be deployed in order to expedite the recovery process and ensure uninterrupted operations. The organization should regularly monitor these levels in addition to the scheduled backup intervals. Regular drills for data recovery and the establishment of backup communications should also be conducted in case communications are disrupted in the future.

KRI 10: Isolation of Control Systems

Parameter:	Isolation of control systems in terms of connectivity to the internet, physical controls, protection, and vulnerability.
Risk Description:	Control systems consisting of multiple levels (levels 0-6; physical, protection, automation, access, SCADA, perimeter, people) that are connected to enterprise or other networks are vulnerable to malware attacks having their systems affected. Black Energy 3 (BE3) malware made its way into the Ukraine enterprise systems through the use of social engineering including other vulnerable control methods.
Measurement of Risk Driver:	- High: Lowest level of layer-based security, more controls, and devices connected through a network/Internet including systems being outdated with older firmware (0 or 1 levels). Less awareness from users (people) and lack of user design protection settings - Medium: Partially layer-based security ranging from a certain amount of controls (3 levels or more), alarms set up for control systems and preprogrammed to trigger for breaker action, password changes, and critical events.

	- Low: The highest level of layer-based security, including most if not all controls isolated and/or not connected to a network solely operational (6 levels). Includes fully set alarm control system for various triggers, and logging system used to determine how certain problems occur after events and prevent them from happening again (including vulnerabilities and cyber attacks)
Data Collection:	**Source:** - Internal diagnostics and continual memory scans - Logs for alerts, incidents, and events within systems and networks - Whitelisted malware protection lists - Physical security checks: obstacles, borders, visible signs, visible cameras - Alerts/alarms measuring detective and defensive measures
Rationale:	Network attacks are common breaches and have a significant impact on a business' network system and infrastructure. The BE3 attack on Ukraine performed on the network and provided a backdoor opportunity for hackers into the rest of the corporate network. With isolating control systems, especially through segmented networks, the Defense-in-Depth strategy takes place and is key for preventing and minimizing attacks toward control systems that are connected online. A layer-based security model would allow security controls to be monitored efficiently increasing the detection rate of attempts to circumvent the security system. Thus, allowing attacks to also be isolated and minimized allowing the rest of the devices to operate which would have gone hand-in-hand with the BE3 attack.
Action Plan:	If deemed necessary for control systems to be connected through networks/Internet, create segmented networks through the use of firewalls and use communication cryptography to protect data helps in aiding against malware (levels 0-6). Otherwise, other action plans include allowing the control system to operate offline (disconnected from the Internet) and operate solely, isolating control systems found behind firewalls from the business network (firewall access control list) to whitelist certain traffic criteria. Enable the use of VPNs if remote access is needed.