PRE-FILED DIRECT TESTIMONY

OF SEAN M. CLEVERLY

ON BEHALF OF NORTHWESTERN ENERGY

TABLE OF CONTENTS

Witness Information

Q. Please provide your name, employer, and title.

A. My name is Sean M. Cleverly. I am NorthWestern Energy's ("NorthWestern") Director of Enterprise Architecture and Cyber Security Officer.

Q. Please provide a description of your relevant employment experience and other professional qualifications.

A. I have over 30 years of experience with NorthWestern in the Business Technology Department (Entech Inc., The Montana Power Company ("MPC"), and finally NorthWestern).

I have a varied background in many business technology disciplines, which gives me a unique perspective of the entire technology ecosystem. However, specifically related to cyber security, I have experience in network architecture to include firewalls both internal as well as external, local area networking, wide area networking, as well as wireless networking. I have experience with remote access technologies for employees, contractors, and small town offices using the Internet. I was involved with the divestiture of MPC, NorthWestern's purchase of MPC, as well as the purchase of hydro system from PPL Montana. Other security specific technologies I have responsibility over include the implementation of network access controls, Internet content filter, intrusion detection, intrusion prevention systems, network vulnerability scanning automation, network segmentation design and implementation, micro-domains, multi-factor authentication, and data loss prevention technologies. I also have responsibility over projects where architecture and security were essential in the initial design, such as the hydro acquisition, wind generation acquisitions, critical infrastructure protection program, the take-over of the security for the electric management system environment, Advanced Metering Infrastructure ("AMI") and Advanced Distribution Management

System architecture, Aberdeen and Glanzer generation station network secure architecture, and Disaster Recovery & Incident Response Planning.

Purpose and Summary of Testimony

Q. What is the purpose of your testimony in this docket?

A. My testimony will focus on the role Business Technology, specifically my team and I, plays in cyber security at NorthWestern and the challenges we face. The threats faced by this sector and our company are significant, and our ability to identify, detect, defend, remediate, and respond to them is crucial. To provide safe and reliable service to our customers, we must be agile, diligent, and invest in the necessary tools such as network layer seven firewall systems, and network-based artificial intelligence engines. These tools allow us visibility, detection, and prevention of threats to preserve the confidentiality, integrity, and availability of our systems. Threats do not take a vacation so this is a 24/7/365 job that demands we have access to threat notifications, alerts, and alarms, which puts us in a position to respond appropriately.

Q. Please summarize your testimony.

A. My testimony describes the implementation of NorthWestern's Cyber Security initiatives and their associated costs as well as our general approach to cyber security and threats that we are exposed to.

Implementation of Cyber Security Initiatives

Q. Please describe how NorthWestern's Business Technology Department implements its Cyber Security programs.

A. Each year, we develop a work plan for security-specific projects like firewall upgrades or replacement projects based on approved capital or expense requests. We also work with the other Business Technology leaders to determine what projects they have requiring involvement of the Security Team. Before implementing a new technology, we clearly define the problem to be solved and identify what part of the CIA (Confidentiality, Integrity and Availability) Triad needs to be addressed. Once the problem is defined and understood, we perform an exercise trying to anticipate what may come next and make sure our proposed solution positions us for what may come next.

It is important to know we also depend on a host of standards, government agencies, and frameworks to help guide our strategy. Those include, but are not limited to, the Center for Internet Security, Department of Homeland Security, The National Institute of Standards and Technology, as well as the International Organization for Standardization.

Q. Why are those initiatives important to ensure NorthWestern provides safe and reliable service to customers?

A. My role is not limited to cyber security; my role as part of NorthWestern, where I lead a team of people who, amongst other duties, perform cyber security functions is to ensure safe and reliable service to our customers. While cyber security is our primary responsibility, we understand what its purpose is within our environments. Our team knows providing safe and reliable service to NorthWestern customers is paramount. Just as the utility network for delivering power is resilient and reliable, our information systems and industrial control systems are designed to provide reliable access and ensure the integrity and accuracy of the data is correct.

Almost every project that NorthWestern pursues has a technology component to it. Every computer, server, tablet, cell phone, camera, switch, router, printer as well as every application a user accesses has been vetted at some point by the Security Team at NorthWestern.

The challenge of protecting these systems is growing exponentially as the demand for utility system automation increases. Customer preferences change on how they want their information delivered. Mobility demands are key to managing a workforce efficiently. Systems integration and data analytics start to drive business decisions. Entering into new markets and transforming traditional business lines while allowing users to work from home have moved the traditional boundaries of security. NorthWestern has over 5,000 devices on our data network(s) and this is increasing daily, and we have over 5,000 applications in our environments. These devices and applications carry with them maintenance requirements such as upgrades, patches, and special configurations, all of which require time and money to support. We also provide security for Internet of Things ("IoT") devices on our leased public/private networks, such as the one used for AMI. The number of end points associated with these devices approaches 600K. One analogy we use is that while previously a castle (the crown jewels of our network(s)) and moat (a traditional security device such as a firewall) strategy may have worked, this strategy is no longer viable. Simply put, there is too much integration, mobility, third-party access, and other requirements for the traditional strategy to be effective anymore. The attack surface, which consists of any device, application, or user accessing our networks, has increased opening a myriad of new threat vectors for nefarious threat actors. Protecting these systems to ensure safe and reliable energy delivery is vital.

Q. What threats does NorthWestern's Business Technology Department face?

A. The threats change on a daily and even hourly basis. On any given day, we encounter one or even all of the examples listed below. It is also important to understand that most of these attempts do not really have names or success. While not successful today, we must still be vigilant.

- **Phishing and ransomware** currently remain the top two classified root causes for data compromises. Publicly available information cites "unknown" as the largest attack vector. This is when an organization discloses a breach but does not determine the root cause. This lack of transparency in the notices makes it difficult to categorize or name every threat.
- **Malware** to include ransomware, payloads in phishing emails. Types of malware we face include, but are not limited to, WannaCry ransomware, CryptoLocker ransomware, Stuxnet worm, and ILOVEYOU worm. Malware is generally delivered in a phishing email with malicious content. We see phishing attempts and emails containing malicious content every day on our email filter systems. In fact, our email filters drop between 85-90% of total email sent to user.user@northwestern.com every day.
- **Code injections** such as Rootkits. Rootkits are installed inside legitimate software, where they can gain remote control and administration-level access over a system. For example, the SolarWinds, SunBurst (malware) attack resulted from malicious code injected into the Orion platform. This is a great example of how these attacks can affect NorthWestern. As a result of the breach to the SolarWinds' Orion platform, NorthWestern was forced to replace its

installation of SolarWinds with a different solution. The replacement solution took over a year to fully implement. Although NorthWestern was not compromised in the Solar Winds Orion platform breach we were compelled to replace the platform.

- **Structured Query Language ("SQL") injections**. These attacks are data driven and could be introduced by completing a form on an unsecure website. Some examples are the Sony, British Royal Navy, PBS, and Yahoo breaches. Stolen data could be anything from personnel records to logon credentials. These types of attacks have not happened to us on our website but have happened to our users going to other websites.
- **Cross-Site Scripting** which is an attack that injects malicious scripts into content from reliable websites. The malicious code joins the dynamic content that is sent to the victim's browser from a legitimate website. Recent examples of this we have seen are Log4j, Java, and HTML exploits.
- **Zero-Day Exploits** which are new vulnerabilities found before patches are released by a manufacturer, generally occur in a browser like Internet Explorer.
- **Man-in-the-Middle exploits** occur when an attacker intercepts a two-party transaction, inserting themselves in the middle. From there, cyber attackers can steal and manipulate data by interrupting traffic. These are network level attacks. The most common avenues for this

type of attack are public Wi-Fi, and poorly configured security devices or computers. A nation-state actor can exploit those avenues to attack a larger target such as a utility company. We see these attempts regularly where a computer gets redirected to a fraudulent website creating a possible connection back to our network(s), or when a computer in someone's home is compromised and an attack is launched from an unknowing individual's computer.

- **Denial-of-Service attacks** work by flooding systems, servers, and/or networks with traffic to overload resources and bandwidth. The result renders the system unable to process and fulfill legitimate requests. In some cases, these attacks overwhelm a system making it vulnerable to further attacks. This attack is very common where a computer packet (series of information) is delivered to a firewall out of sequence in hopes the firewall will allow the out-of-sequence packet.
- **Internet-of-Things (IoT)[1] attacks** are becoming more popular due to the rapid growth of IoT devices and (in general) the low priority given to embedding security in these devices and their operating systems by the manufacturers. As an example, a Las Vegas casino was attacked by a hacker gaining entry via an Internet-connected thermometer inside one of the casino's fish tanks. From there, the threat actor was

[1] IoT devices are machines placed on a network and given an address so they can be communicated with.

able to move laterally in the network and access things on their network. We see IoT devices on our network “phoning-home” or communicating to outside vendors all the time such as printers communicating maintenance information and postage meters communicating usage information, to name a few.

- **Nation-State attacks** on U.S. critical infrastructure. Nation-State threat actors typically (but not always) come from the "big four”: China, Russia, North Korea, and Iran. Each government has different structures, circumstances, and motivations that define the form their activity takes against the U.S. These attacks and who is behind them are often credited to a specific group based on the characteristics of the attack. The Colonial Pipeline Attack was credited to an organization operating in Eastern Russia known as DarkSide. The root cause of that attack was stolen administrative credentials on a virtual private network (VPN) server.
- **Insider Threats** are most often overlooked. These come in four types: oblivious, negligent, malicious, and professional. We address these threats with training, least privilege access, data-loss-prevention tools, and account management. The oblivious or unaware user and the negligent user are our most common threats. In 2021, human error represented 87% of data compromises. During our website upgrade, one of our vendors missed configuring one of our applications with the proper controls to block an automated process to fill out forms on our

website. This resulted in a high number of forms being filled out in a short period of time. This activity was quickly discovered and that site brought offline while the vendor remediated the page.

As is apparent from these examples the breach or attempted breach can result from anything or anyone connected to a network. We have third-party contractor access, malicious and non-malicious website activity as well as software and hardware which can be armed with malicious code. Supply chain issues have gained notoriety since the SolarWinds breach. This was a legitimate platform breached at SolarWinds. Malicious code was loaded into the Orion platform (used to distribute updates and patches to customers) and was legitimately installed on customers' networks. Given the current geo-political climate and the Cybersecurity and Infrastructure Security Agencies (CISA) Shields Up guidance, cyber space is a hostile environment and any device on any network must be considered a potential threat.

Q. How does NorthWestern respond to these threats?

A. Each of the threats mentioned presents a unique set of challenges. Complications ensue because most threats can present themselves in a multitude of ways. We leverage our tools, correlate events, monitor security events throughout the world, and perform hygiene. The team is constantly educating themselves on emerging threats and monitoring for anomalies.

We have a mature cyber component within the disaster recovery and incident response plan which we use for all incident response. The plan is exercised and reviewed at a minimum on an annual basis.

Q. How does the Business Technology Department address those threats?

A. As previously stated, the complexity and variety of cyberattacks continues to increase and there is no end in sight. There are different types of attacks for every nefarious purpose. While cyber security prevention measures differ for each type of attack, good security practices, education, visibility, and basic IT hygiene (patching) are generally a good start at mitigating these attacks.

In addition to implementing industry best cyber security practices, we exercise secure coding practices, keep systems and security software up to date, leverage firewalls, threat management tools and solutions, install antivirus software with artificial intelligence engines across systems, control access and user privileges, backup systems often, segment our networks, and proactively watch for and receive alarms on breached systems.

Q. Given the evolving and increasing nature of cyber security threats, how does NorthWestern plan to protect its system from future threats?

A. NorthWestern's current strategy of ensuring least-privilege access (giving people just the appropriate access to perform their jobs), enforcing good hygiene, patching, monitoring and alerting, threat hunting, providing visibility by having access to logs, educating, following best practices while continuing our secure defense in depth, micro segmenting, and finally continuing to be hyper vigilant with cyber climate will allow us to make timely and appropriate investments in technology and be positioned for success. It is important to understand that these investments in technology are the key to being able to continue to defend our cyber assets.

Cyber threats are always going to evolve, which is why we focus on enhancing visibility, alerting into and out of our critical control systems, and improving awareness for emerging threats.

Costs of Cyber Security Initiatives

Q. How much did NorthWestern spend on its Cyber Security efforts during the 2021 test year?

A. NorthWestern spent $3,249,600 on Cyber Security efforts in 2021.

Q. **Please explain how the costs of NorthWestern's Cyber Security efforts have changed from year to year since NorthWestern's last rate reviews.**

A. See the table below.

	Cyber Security Maintenance and Subscription Costs	% Cyber Security from Prior Year
2017 Actual	$1,847,804	2.8%
2018 Actual	$1,937,451	4.7%
2019 Actual	$1,830,282	-5.7%
2020 Actual	$2,430,301	28.2%
2021 Actual	$3,249,600	28.8%
2022 Forecast	$4,212,467	25.8%
Average % Difference Year Over Year		14.1%

Q. **Does NorthWestern expect the trend of increased Cyber Security costs to continue into the future? If so, why?**

A. Yes, I would expect costs for Cyber Security at NorthWestern to continue to increase. I fully expect general Information Technology costs to increase so it is only logical to assume Cyber Security costs will increase. Cyber security is not a destination, it is a journey, and as threats evolve and become more sophisticated our tools and even our approach need to evolve also. As automation and cloud computing become prevalent, the threats we face become more complex and the security surface expands, which, all told, causes costs to continue to increase. Maintaining the technologies we have on our networks and the tools used to access those networks is critically important, and those tasks alone have significant costs associated with them.

Q. Can you quantify what those costs are expected to be?

A. No, I cannot accurately predict what those costs will be. While we clearly see a trend with the rising costs of Information Technology in general and costs associated with Cyber Security, there are factors we cannot predict such as acquisitions, third-party breaches (those are breaches of our supply chain vendors), and finally government regulations that may require additional cyber security investments.

I do think that our projected costs demonstrate our commitment to spend wisely. While the costs are expected to continue to increase, we have demonstrated the ability to plan for and anticipate the tools required to continue to provide industry best practice protection while aggressively providing first class threat hunting capabilities.

Q. Does this conclude your testimony?

A. Yes, it does.

VERIFICATION

This Pre-filed Direct Testimony of Sean M. Cleverly is true and accurate to the best of my knowledge, information, and belief.

/s/ Sean M. Cleverly
Sean M. Cleverly