Teaching Case

JITTC

Journal of Information Technology Teaching Cases
2023, Vol. 0(0) 1–11

DOI: 10.1177/20438869231155934
journals.sagepub.com/home/jittc
SAGE

Code red: A nuclear nightmare-navigating ransomware response at an Eastern European power plant

Namita Madhira, Justin M Pelletier, Daryl Johnson and Sumita Mishra

Abstract

Over the past decade, the number and scale of ransomware attacks has grown. These attacks have stretched across multiple industries globally and caused billions of dollars of damages. Recent attacks have disrupted critical infrastructure and have served as prelude to war. Studies have shown that there is a lack of awareness among industry practitioners surrounding appropriate responses to ransomware. This failure during a career-defining moment is largely due to the gap between cyber security academic knowledge and industry practice. We therefore provide a learning resource for ransomware response education that is academically adequate, practically viable, and ultimately illustrates a process for proper employment of technology. This case, exposes students to technical requirements for a ransomware response and explores ransomware best practices. Discussion questions and a wargaming-style purple team exercise for individuals or groups extend the opportunity for delivering additional technical depth.

Keywords

cybersecurity, ransomware, management information systems, teaching cases, crime and security, IT for competitive advantage

Scenario

At 5:00 a.m. on a cold winter morning in an undisclosed East European nation, Arya, the senior security lead at The Nation nuclear power plant, woke up with a feeling of dread. With cyberattacks on the rise due to the tensions of war, she planned to run an incident response simulation today as a practice exercise for her team. The exercise had to be successful. With the previous attempts failing under her watch, this was Arya's last attempt to save her job.

Even the sunrise and the sounds of birds chirping in the distance could not calm Arya's preoccupied mind. With a steaming mug of strong coffee, she sat at her desk at home and switched on her laptop in order to gather her thoughts and plans for the exercise. With war tensions, Arya was aware of the looming threat of advanced persistent threat (APT) groups like Cozy Bear (APT29). Cozy Bear was known to target European and NATO member countries and the energy industry as well. Their primary attack tactics begin with large-volume spear phishing campaigns that would deliver an extensive range of custom compiled malware binaries. APT29 typically makes use of PowerShell and Windows Management Instrumentation (WMI).

After reading the news about the ransomware attack that had affected the United States-based Colonial Pipeline company in 2021, she keenly followed the development of the situation and even prepared detailed notes about it. Wanting to model her incident response exercise around a similar situation, Arya decided to go over the details of the Colonial Pipeline attack.

In true journalistic style, Arya's notes first presented a high-level brief of the attack:

> The Colonial Pipeline is an American oil pipeline system originating in Houston, Texas, that is responsible for the supply of about 45% of all the refined petroleum to the U.S. East Coast market. Comprising more than 5,500 miles, it is one of the largest and vital oil pipelines in the United States (Colonial Pipeline Company, 2021).
>
> On May 7, 2021, the Colonial Pipeline company fell victim to a ransomware attack causing it to shut down for nearly one week.

Department of Computing Security, Rochester Institute of Technology, Rochester, NY, USA

Corresponding author:
JM Pelletier, Computing Security, Rochester Institute of Technology, 20 Lomb Memorial Drive, Rochester, NY 14623, USA.
Email: jxpics@rit.edu

This shutdown affected several consumers of gasoline, home heating oil and jet fuel along the U.S. East Coast. The attack was deemed as a national threat and caused President Joe Biden to declare a state of emergency.

A group known as DarkSide were identified as the attackers. The attackers demanded a ransom of 75 bitcoins (approx. $4.4 million as of May 7, 2021).

Arya then moved on to her notes on the cause of the Colonial Pipeline attack. This was so that she could determine if this could also potentially be a weakness in her company.

The root cause of the Colonial Pipeline attack was determined to be a compromised password. On June 8, 2021, Charles Carmakal, senior vice president and CTO of security firm Mandiant revealed that the attackers got into the Colonial Pipeline network through an exposed password for a Virtual Private Network (VPN) account. The VPN account, that belonged to an employee, was unused, but active at the time of the attack (Endler, 2021). According to Mandiant, the password was relatively complex and likely would have been difficult for the attackers to guess. A report by Bloomberg (Turton and Mehrotra, 2021) stated that the password was discovered inside a batch of leaked passwords on the dark web, suggesting that the employee had reused the password on an account that was compromised during a different data breach. However, Mandiant said that it is uncertain that this was how the DarkSide attackers obtained the credentials (Lakshmanan, 2021). The VPN account has since been deactivated.

Arya noticed that the VPN account did not use Multi-Factor Authentication (MFA), making it easier for the attackers to breach the Colonial Pipeline network with just the VPN login credentials. Her company, The Nation nuclear power plant, had recently rolled out a multi-factor authentication policy within the entire company.

The group behind the ransomware attack had been identified as DarkSide, the cyber criminals who had founded the Ransomware-as-a-Service (RaaS) concept. The RaaS business model involved ransomware operators and affiliates. The operators, often cybercrime groups, interview and then distribute their ransomware code to affiliate hackers in exchange for a fee or a percentage of the royalty.

In the Colonial Pipeline attack, DarkSide employed a double extortion strategy. This involves exfiltrating a victim's sensitive data first and then encrypting it. An investigation by Trend Micro Research (Trend Micro Research, 2021) provides a look into how the DarkSide ransomware group operates. The details of the attack phases identified to have been used by DarkSide is depicted in Figure 1.

The ransomware attack impacted the Colonial Pipeline company severely. Firstly, the attackers were able to steal 100 gigabytes of data within a two-hour window and threatened to leak the data if the ransom was not paid. According to CNN (Bertrand et al., 2021) the billing system of the Colonial Pipeline was compromised. This prompted the Colonial Pipeline company to shut down in order to contain the threat and prevent further attacks. The Colonial Pipeline was forced to halt all activities for 5 days. Additionally, the goal for attackers in a ransomware attack is to have the victim pay a ransom, which is exactly what Colonial Pipeline did. They paid the 75 bitcoins (approx. $4.4 million at that time) ransom. At the time the ransom demand was made, Colonial Pipeline CEO, Joseph Blount said that it wasn't clear how widespread the intrusion was or how long it would take Colonial Pipeline to restore the compromised systems. Hence, Blount decided to pay the ransom, hoping it would speed up the recovery time.

The impact of the Colonial Pipeline attack also extended beyond the cyber security sphere and caused significant and immediate social repercussions:

- It affected the airline industry where the shortage of jet fuel impacted many carriers including American

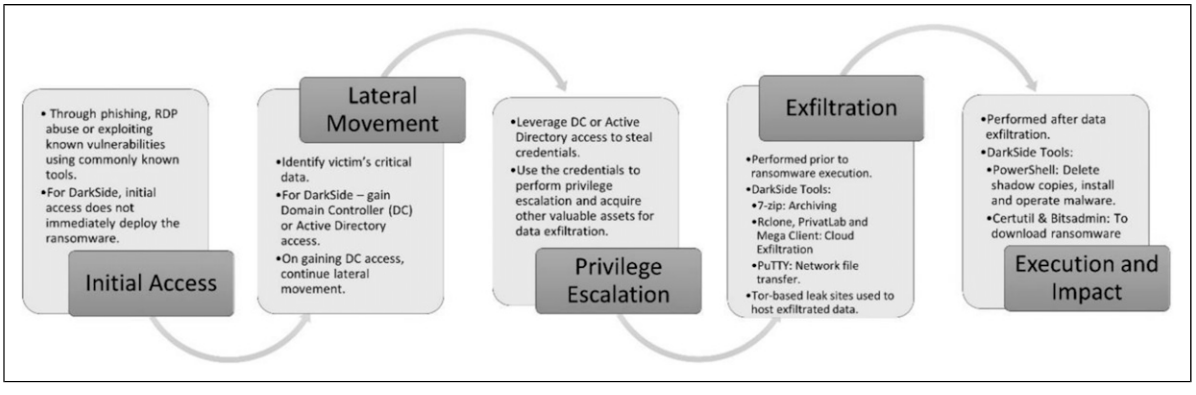

Figure 1. DarkSide attack lifecycle.

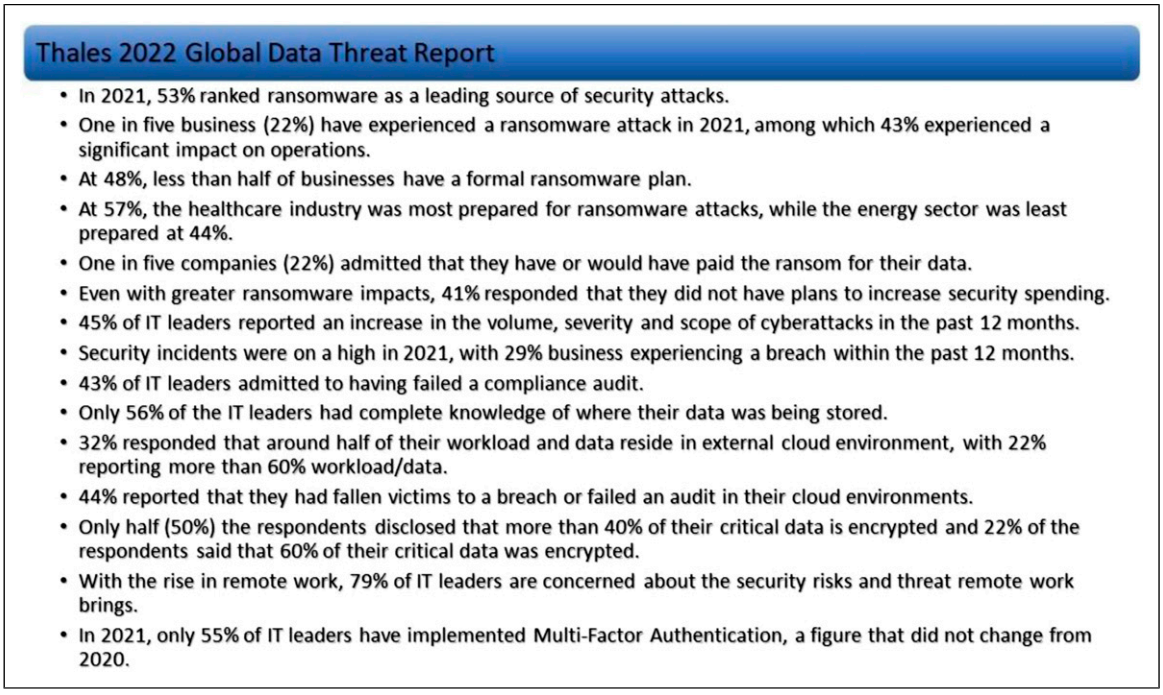

Figure 2. Global data threat report statistics, derived from Thales (2022).

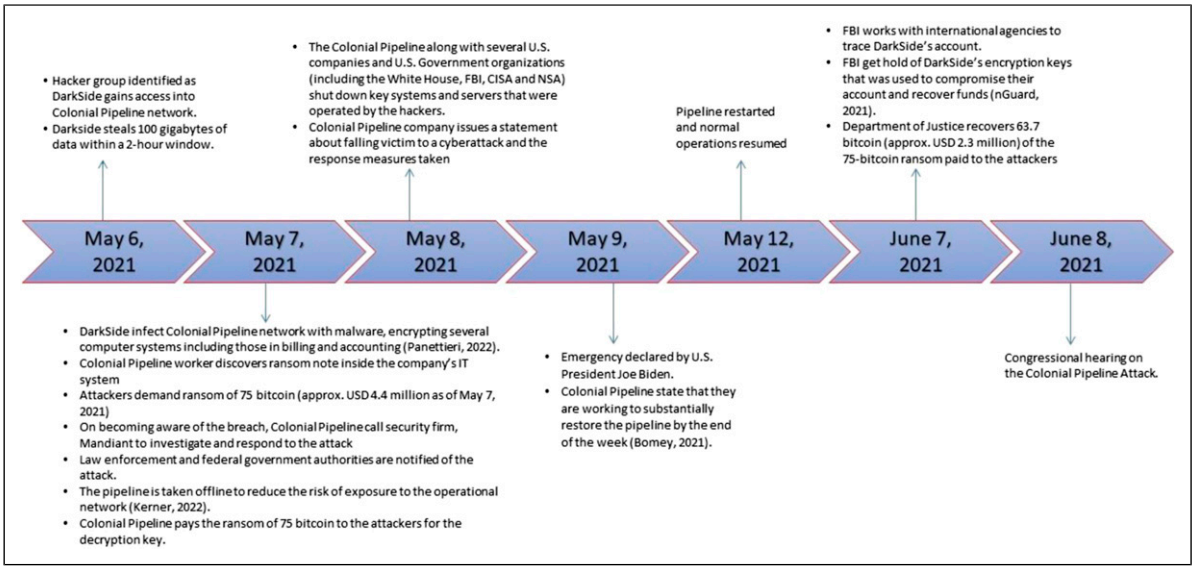

Figure 3. Colonial pipeline attack timeline.

Airlines. There were also limited disruptions at other airports, including Atlanta and Nashville.

- The fear of a fuel shortage caused panic-buying and long lines at fuel stations in many states, including Florida, Georgia, Alabama, Virginia, and the Carolinas. In some states, people even filled plastic bags with gasoline, triggering a U.S. Consumer Product Safety Commission alert, warning consumers to only use containers meant for fuel.
- The panic-buying also led to some real shortages in certain areas as consumers bought more gasoline than usual.
- The transportation industry was affected as several trucking companies had to halt their long-haul

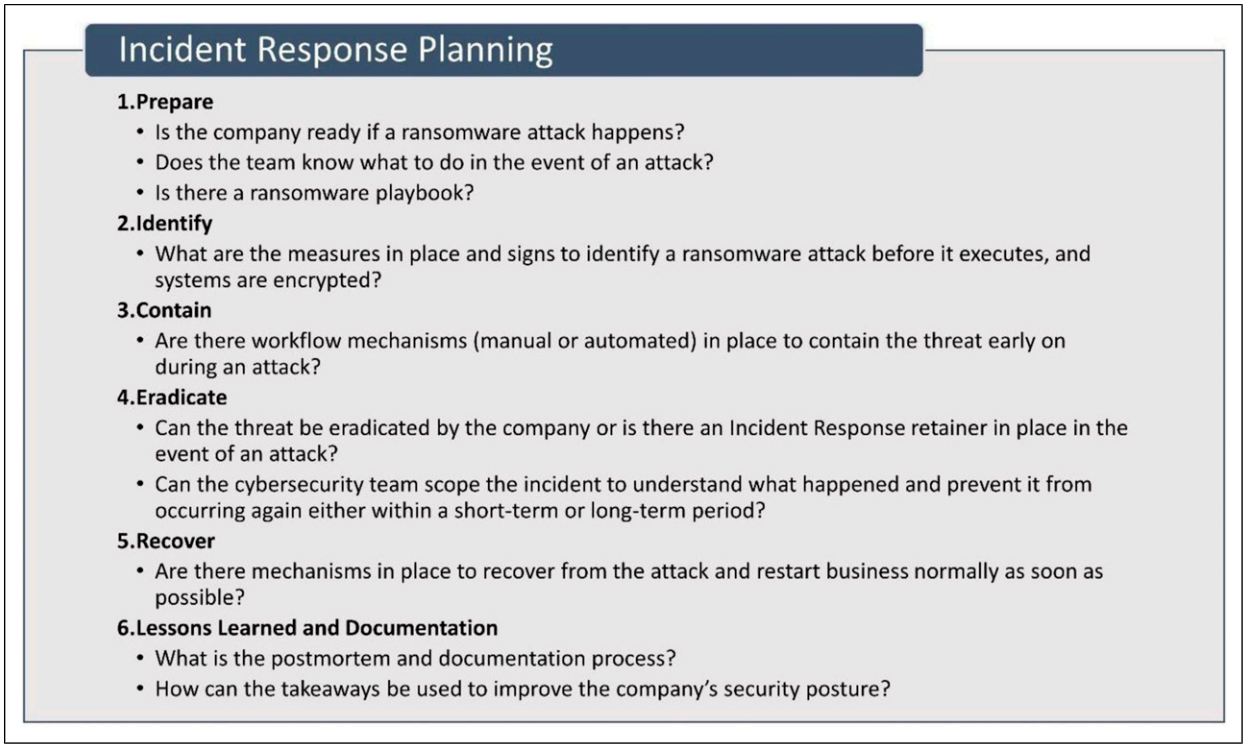

Figure 4. Incident response plan model.

delivery operations out of fear of being stranded with no fuel.
- There was a spike in the average fuel price, with regular fuel topping $3/gallon (Tsvetanov and Slaria, 2021).

There were several lessons to be learned from the Colonial Pipeline attack. It reinforced the importance of cybersecurity in maintaining energy security and the security of critical infrastructure in general. The dire need for a tested incident response plan was highlighted as well as the importance of MFA. The attack also reiterated that remote work and remote access are still a major area of risk. Adding to this, the increase in cloud environment adoption was also a rising risk. These factors have inherently called for more stringent Federal security policies (Borgia et al., 2021).

The aftermath of the Colonial Pipeline attack exposed several vulnerabilities within critical infrastructure. It served as a wakeup call for businesses, for other critical infrastructure sectors, and the government (Kannry, 2022). On 12 May 2021, U.S. President Joe Biden signed an Executive Order (Exec. Order No. 14028) on Improving U.S. cyber security (The White House, 2021). This called to action the following:–

- Mandates for Federal agencies to deploy Multi-Factor Authentication (MFA) and encryption within a specific period of time and move to secure cloud services and zero-trust architecture.
- Establishing a baseline of security standards for development of software sold to the government.
- Establishing a Cybersecurity Safety Review Board that convenes after a significant cyber incident and makes recommendations for cybersecurity improvement.
- Creating cyber security event log requirements for federal agencies.
- Improving security detection on federal networks and information sharing within Federal agencies.
- Creation of a standardized Incident Response playbook for federal departments and agencies.

Other significant events that took place in the wake of the Colonial Pipeline attack were as follows:

- Chairman Richard Glick of the Federal Energy Regulatory Commission released a statement (FERC, 2021) calling for an examination of Mandatory Pipeline Cybersecurity Standards.
- The Cybersecurity and Infrastructure Security Agency (CISA, 2021) setup "stopransomware.com", a catalog of ransomware-related resources and information on known exploited vulnerabilities that companies can use to protect themselves.

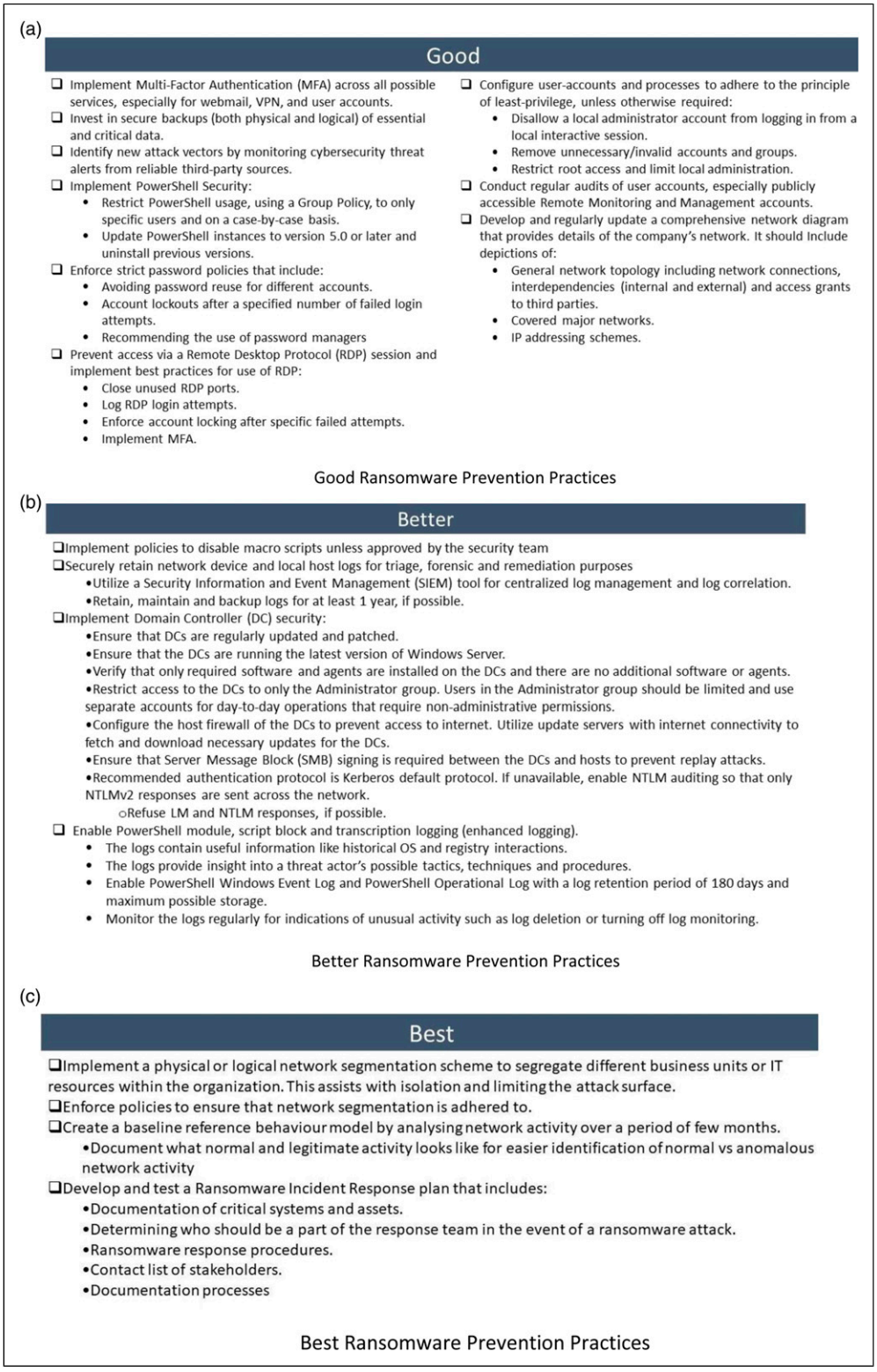

Figure 5. (a): Good ransomware prevention practices. (b): Better ransomware prevention practices. (c): Best ransomware prevention practices.

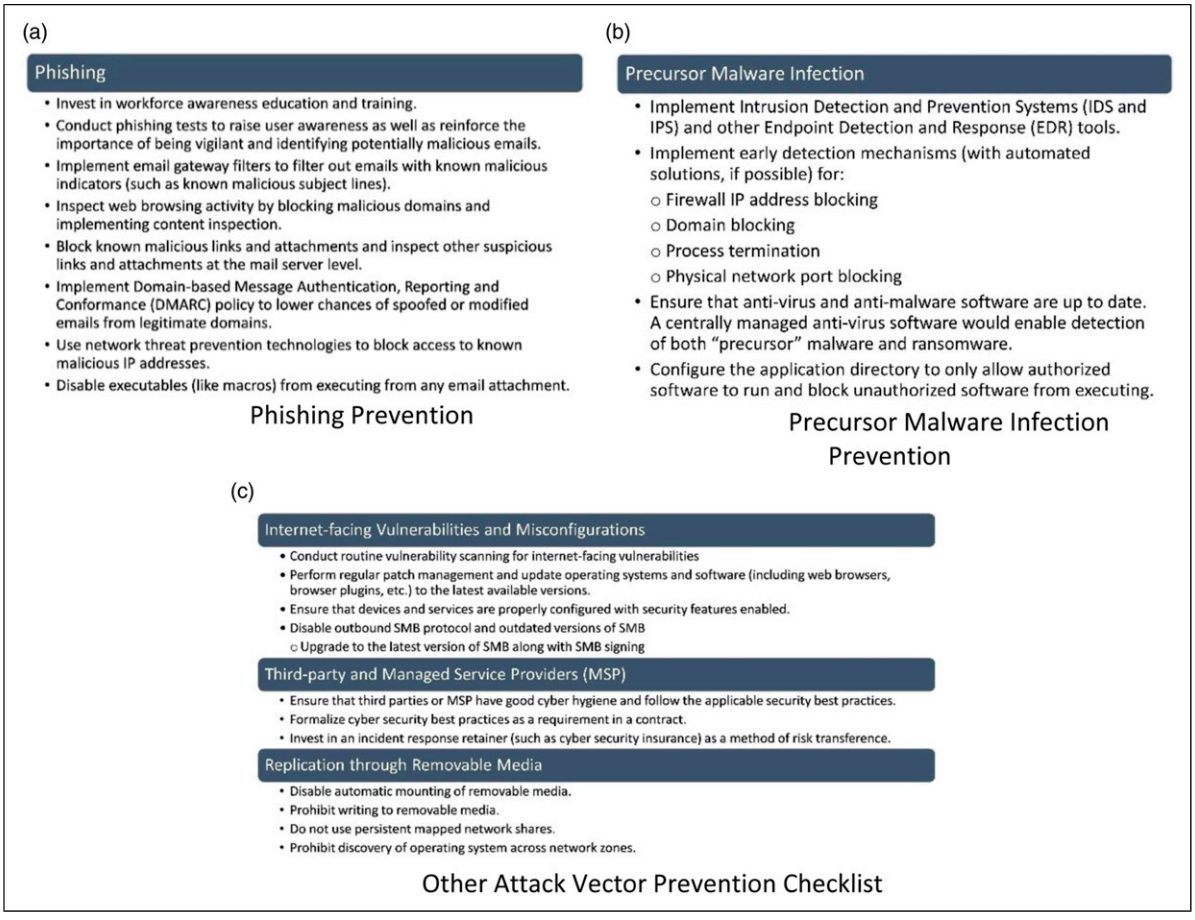

Figure 6. (a): Phishing prevention. (b): Precursor malware infection prevention. (c): Other attack vector prevention checklist.

- A Global Data Threat Report by Thales uncovered details about global organizations affected by ransomware (Thales, 2022). The research survey was conducted by the group 451 Research and included more than 2700 IT decision-makers in various business industries, worldwide. Some significant details of the research are depicted in Figure 2.

The final note Arya had on the Colonial Pipeline attack was a detailed timeline of significant events that had occurred at around that time. Arya created the timeline depicted in Figure 3. It provided a detailed picture of events such as when and where the attack began (Panettieri, 2022), when the colonial pipeline was taken offline (Kerner, 2022), when it was restored (Bomey, 2021), recovery of the ransom (nGuard, 2021) and more.

Ransomware playbook

Once she was done reviewing the Colonial Pipeline attack details, Arya went over the plan for today's exercise. She planned to launch this exercise as a surprise to her team, just like a real cyber incident. In preparation for the simulation, Arya updated the purple team exercise plan that her company developed some time ago. In addition to this, she had also reached out to a cybersecurity expert, Daniel, a few days ago, for some ideas and advice. Daniel had sent over a ransomware playbook (CISA & MS-ISAC, 2020; Rapid7, 2021) that detailed best practices. Arya had spent the past 2 days going through the documents and adapting them in accordance with the laws of her country and power plant regulations set by the government.

The ransomware playbook also contained information on ransomware best practices. In preparation for the mock exercise, Arya had thoroughly reviewed the playbook and prepared notes that summarized the best practices. She categorized it into 2 sections, "prevention" practices and "mitigation and response" practices. Arya's first focus was ensuring that The Nation power plant satisfied as many prevention criteria as possible before moving to mitigation and response.

The cyber security team at the power plant was a smaller one consisting of 3 security analysts, 2 security engineers,

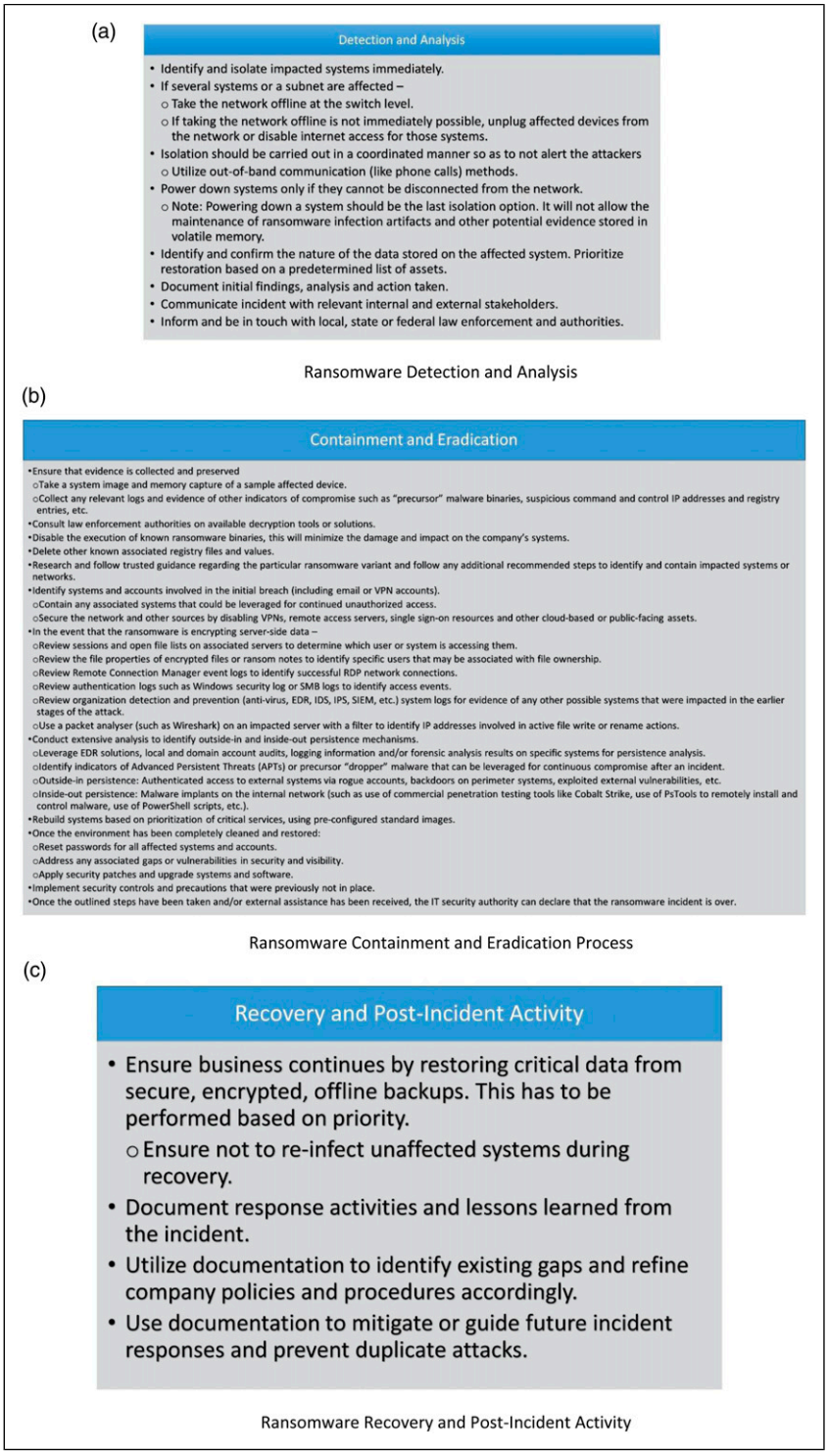

Figure 7. (a): Ransomware detection and analysis. (b): Ransomware containment and eradication process. (c): Ransomware recovery and post-incident activity.

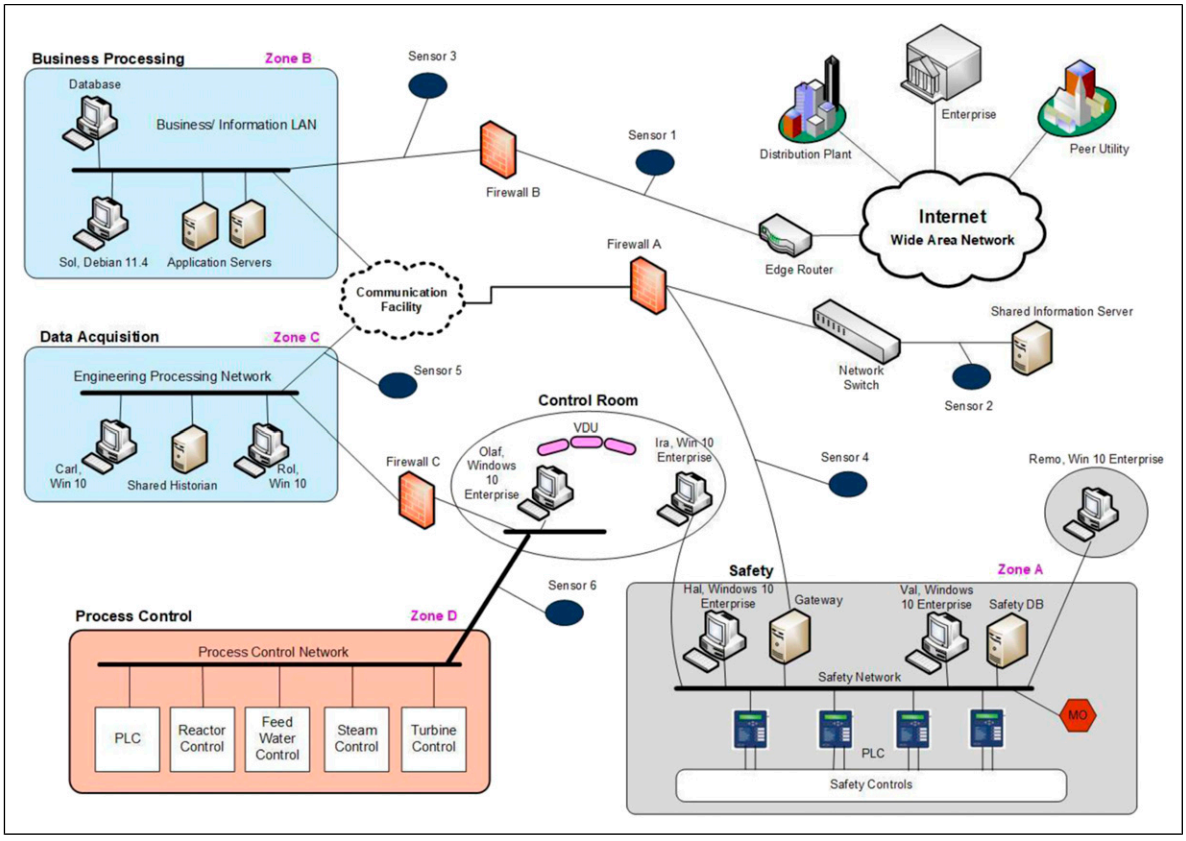

Figure 8. The network diagram for Arya's nuclear power plant.

1 data privacy and risk analyst, and Arya, the senior security lead. The team had ensured that the plant was equipped with a considerable amount of cyber security controls, especially those laid out in the nuclear plant cyber program. This included the following:

1. Multi-factor authentication on all local accounts.
2. Adhering to government compliance policies.
3. Documentation of critical infrastructure.
4. A developed incident response plan
5. Access control mechanisms.
6. Use of vulnerability scanning, SIEM and EDR solutions.
7. Cloud data back-ups.

Though the power plant had a cyber incident response plan that followed the suggested model depicted in Figure 4, it was only recently developed and never actually been tested to see if it is practical and usable for various cyberattacks. This was a goal Arya wanted to achieve with today's simulation.

Prevention. The "prevention" document first listed out many general best practices for ransomware prevention. Arya took some time to classify these practices into "good," "better," and "best" practices, based on what her company had implemented and what she perceived to be "easier to implement." Arya's classification for "good" practices, depicted in Figure 5(a), consisted of controls her company had mostly implemented and in Arya's opinion, were the easiest to implement. The "better" controls, depicted in Figure 5(b), were moderately time consuming to implement and the "best" controls, depicted in Figure 5(c), were the most difficult or time consuming to implement. Over the course of the mock exercise, Arya would be monitoring which practices were already in place and what needed to be included.

Once Arya was satisfied with her classification, she moved on to her next focus—known ransomware attack vectors. In the exercise, Arya wanted to focus on the attack vectors that were noted weaknesses within the power plant. Since some of the plant engineers weren't careful when it came to email vigilance, Arya's first priority was to check all the boxes in the phishing prevention practices laid out in Figure 6(a). Following this, Arya's next focus was to make certain that all their monitoring and response tools were up to date and correctly configured and by extension, checking all the boxes to prevent precursor malware infection (depicted in Figure 6(b)). Third and final on Arya's prevention outcomes from the ransomware mock attack were ticking as many boxes as possible in Figure 6(c) checklist,

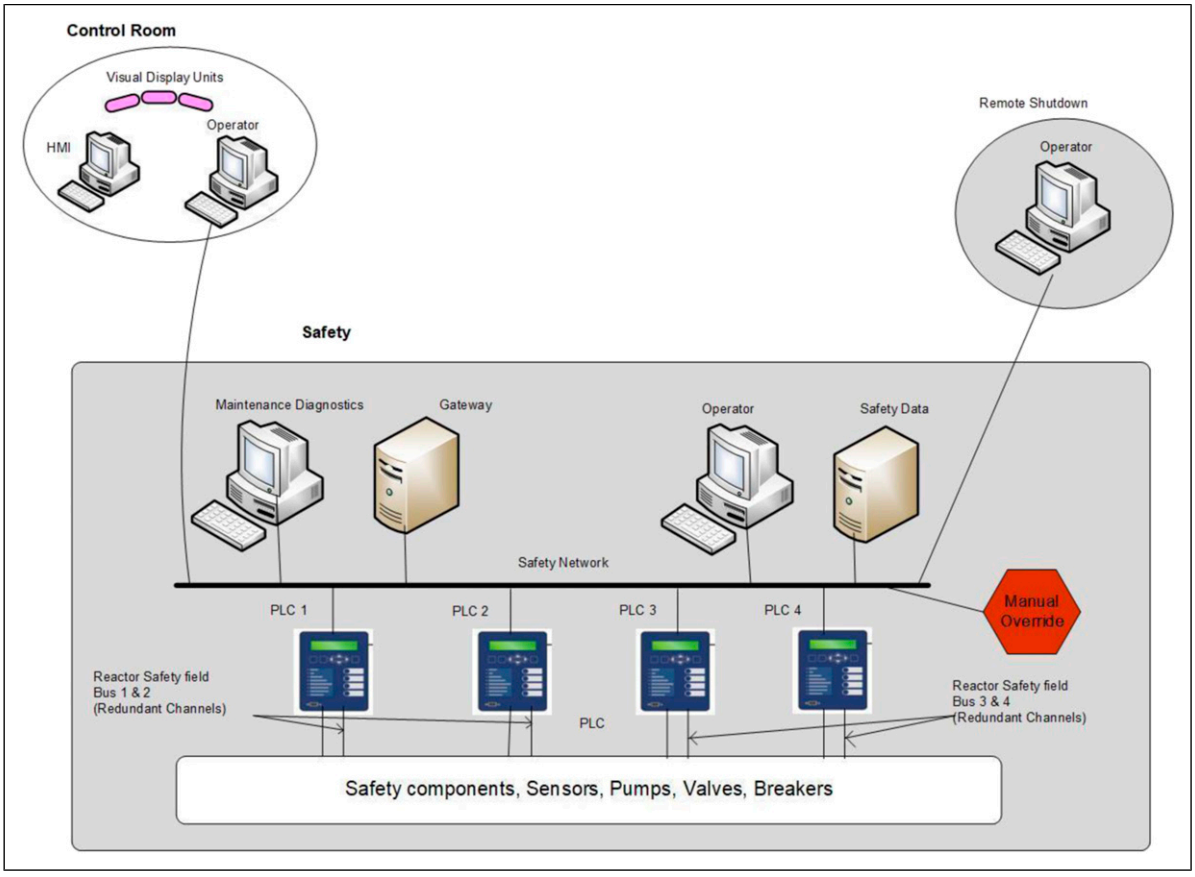

Figure 9. The safety and control room for Arya's nuclear power plant.

the one which she was confident that there were not many The Nation nuclear power plant was missing.

Mitigation and response. When it comes to ransomware mitigation and response, the first step is to detect which systems and which part of the network has been impacted. The detection and analysis process was highlighted in Figure 7(a).

Once detected, the next step is to safely contain the malware and eradicate it from the environment. This is the most time consuming and detailed process. Arya's notes on this procedure are detailed in Figure 7(b).

The final step in the mitigation and response procedure is to instill normalcy and ensure business continuity. The recovery and post-incident activity steps are outlined in Figure 7(c)

Through the exercise, Arya was keen to see what her team's stance on paying a ransom would be. From her perspective, she knew that it is highly recommended to avoid paying the ransom and first investigate alternative recovery methods. Paying a ransom does not guarantee that the attackers will provide a working decryption key or that they will not release the company's data.

The power plant

The Nation's nuclear power plant, one of the oldest in the country, was responsible for generating nearly 60% of the electricity in the country. It made use of a pressurized water reactor (Touran, 2022). The core of the reactor contained all the nuclear fuel and generated all the heat. It comprised low-enriched uranium, control systems, and structural materials. The coolant material, water in this case, passes through the core and is responsible for transferring the generated heat from the fuel to the turbine. The turbine uses the heat to generate the electricity. The containment is the dome-shaped structure made of high-density, steel-reinforced concrete that separated the reactor from the outside environment. Finally, the cooling towers are used to discard excess heat that cannot be converted to energy.

The Nation nuclear power plant's network was redesigned several years ago and now matches the best practices recommended by the U.S. Nuclear Regulatory Commission (USNRC 2012). The network diagram is provided in Figure 8.

Conclusion

With all the documents and plans in order, Arya got ready to leave for work. She took her umbrella with her as she noticed that the gloomy weather had turned to rain, bringing with it a feeling of foreboding. On reaching the nuclear power plant at 8:40 a.m., she headed to the conference room to set up the exercise. At 9:05 a.m., Arya stood up, intending to call the entire cyber security team. As she opened the door to exit the room, she bumped into a flustered and panting plant engineer. With a worried expression, he reported to Arya that the on-duty engineers were unable to access any of the systems in the control room and the human–machine interface for the power plant was locked. The electronic control for the plant's cooling system was shut and the power plant was overheating. If this was not addressed, the core would soon overheat leading to a nuclear reactor meltdown. The only other option, the engineer mentioned, was a manual override of the gate control system. The manual override function was present in the safety zone of the nuclear power plant (Figure 9). Arya knew from her risk management exercise experience that the manual override would deactivate the plant during the annual peak demand cycle and could create a cascading brownout throughout the region.

Panic set in as Arya realized that in an ironic twist of events, she, who wanted to conduct a surprise mock attack simulation today, now had a very real cyber incident on her hands. She now had to run the exercise in a real-life situation, with no time to prepare and immediate response required.

Discussion questions

1. You are Arya. What is the first course of action you would propose to take in this situation?
2. Who should be involved in the cyber security incident operations?
3. Should the company consider paying the ransom? What are the advantages and disadvantages of paying ransom?
4. What components of the existing ransomware playbook allow for effective response in this situation?
5. What, if any, changes or additions do you recommend being made to the playbook?
6. Considering the scenario outlined above, what are the geo-political implications of the situation?
7. What security regulations and compliance targets should the company follow and use to draft their security policies?
8. What do you think has changed in technology that needs to be addressed by organizations and cyber-attack response playbooks?

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Supplemental Material

Supplemental material for this article is available online.

ORCID iD

JM Pelletier https://orcid.org/0000-0002-8330-045X

References

Bertrand N, Perez E, Cohen Z, et al. (2021) Colonial pipeline did pay ransom to hackers, sources now say. CNN. URL. Available at: https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html

Bomey N (2021) Colonial pipeline looking to "substantially restore operations by end of week". USA TODAY. URL. Available at: https://www.usatoday.com/story/money/2021/05/10/gas-prices-colonial-pipeline-ransomware-attack-cyberattack/5019214001/

Borgia M, Jost B, Margaryan M, et al. (2021) Following colonial pipeline ransomware attack, oil and natural gas companies must prepare for new regulations and added scrutiny of cybersecurity programs | Davis wright tremaine. [online] Dwt.com. Available at: https://www.dwt.com/blogs/privacy–security-law-blog/2021/05/tsa-pipeline-cybersecurity-directive

CISA (2021) Stop Ransomware. [online] cisa.gov. Available at: https://www.cisa.gov/stopransomware

CISAMS-ISAC (2020) CISA MS-ISAC Ransomware guide. Available at: https://www.cisa.gov/stopransomware/ransomware-guide

Colonial Pipeline Company (2021) Our company. [online] Colonial pipeline company. Available at: https://web.archive.org/web/20210510235337/https://www.colpipe.com/about-us

Endler D (2021) Council post: one stolen password took down the colonial pipeline — is your business next? [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/09/14/one-stolen-password-took-down-the-colonial-pipeline—is-your-business-next/?sh=4907f5e25f56

FERC (2021) Chairman Glick and commissioner Clements call for examination of mandatory pipeline cyber standards in wake of colonial pipeline ransomware incident. Available at: https://www.ferc.gov/news-events/news/statement-ferc-chairman-richard-glick-chairman-glick-and-commissioner-clements

Kannry S (2022) Colonial pipeline one year later: are critical infrastructure operators more secure? Axio. Available at: https://axio.com/insights/colonial-pipeline-one-year-later/

Kerner S (2022) Colonial Pipeline hack explained: everything you need to know. [online] techtarget.com. Available at: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Lakshmanan R (2021) Hackers breached colonial pipeline using compromised VPN password. [online] The hacker news. Available at: https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

nGuard (2021) Colonial Pipeline – timeline of events. [online] Nguard.com. Available at: https://www.nguard.com/colonial-pipeline-timeline-of-events/

Panettieri J (2022) Colonial Pipeline cyberattack: timeline and ransomware attack recovery details - MSSP alert. [online] MSSP alert. Available at: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/

Rapid7 (2021) Ransomware playbook. Ransomware playbook. Available at: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf

Thales (2022) One in five businesses have paid or would pay a ransom for their data, finds Thales. Available at: https://cpl.thalesgroup.com/about-us/newsroom/2022-data-threat-report-press-release

The White House (2021) Executive order on improving the Nation's Cybersecurity. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Touran N (2022) Nuclear power plants. What is nuclear? Available at: https://whatisnuclear.com/reactors.html#:~:text=Main.components&text=It.contains.low%2Denriched.uranium,the.fuel.to.a.turbine

Trend Micro Research (2021) We know about the darkside ransomware and the US pipeline attack. [online] trendmicro.com. Available at: https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

Tsvetanov T and Slaria S (2021) The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*, *209*, 110122.

Turton W and Mehrotra K (2021) Hackers breached colonial pipeline using compromised password. Forbes, June 4, URL. Available at: https://www.bloomberg.com/news/articles/2021-06-04/hackersbreached-colonial-pipeline-using-compromised-password/

U.S. Nuclear Regulatory Commission (USNRC) (2012) *Secure Network Design. NUREG/CR-7117.SAND2010–8222P.* Albuquerque, NM: Sandia National Laboratories.

Author biographies

Namita Madhira has a Master's degree in Computing Security from Rochester Institute of Technology. This teaching case was written during her Master's degree fulfillment. She is currently working as Cybersecurity Research and Development Engineer. Her areas of interest include usable security, open-source security, and incident response.

Justin Pelletier is the Director of the Cyber Range and Training Center in the ESL Global Cybersecurity Institute at Rochester Institute of Technology (RIT). As a component of this work, he trains and leads student teams to perform security assessments for partner organizations and oversees cybersecurity competitions that bring together the top cyber talent from across the globe. As a Professor of Practice in the Department of Computing Security, Dr. Pelletier teaches at the undergraduate and graduate levels and helped to bring the Hacking for Defense initiative to RIT. He holds a PhD in Information Assurance and Security, an MBA in Entrepreneurship, and a BS in Computer Science. He is also a combat veteran and currently serves as a Major in the U.S. Army Reserve.

Professor Daryl Johnson received his MS in Computer Science from the Rochester Institute of Technology in 1987. He has developed over thirteen and co-developed over a dozen new courses in the networking, security, and systems administration areas as well as redesigning and contributing to many others. He has been involved in the creation of three departments and five degrees including his current department of Computing Security. His attention over the last fifteen years has been focused in the areas of cyber security competitions, visualization of cyber-attacks, Covert Communication, and IoT/CPS/SCADA security. He has authored or co-authored over 60 papers in the cybersecurity field. He created the first course in cybersecurity at RIT in 1998. He has been instrumental in the formation of the Northeast Collegiate Cyber Defense Competition (NECCDC) and the Collegiate Penetration Testing Competition (CPTC). He served as the Red Team Captain for the NECCDC for 14 years since its inception in 2008.

Sumita Mishra holds a PhD in Electrical Engineering and has served as a computing security faculty member at Rochester Institute of Technology for 16 years. She has led and participated in several NSF-funded projects (SFS-Capacity Building, IUSE, ATE) focused on computing and cybersecurity education. She also serves as the department graduate program director and has mentored both undergraduate and graduate students on research. Dr. Mishra is an active member of IEEE and ACM and has published over 70 articles in reputed journals and academic conferences in her field.