Healthcare Data Under Siege: Understanding and Mitigating Cyber Threats for Non-Tech Leaders

1

Presenters from MN Community Measurement

William Muenchow
Vice President of Technology & Security, CISSP, CEH

William is the VP of Technology and Security and has worked in cyber security since 2004 and holds multiple InfoSec certifications.

Jeremy Griggs
Technical Support Specialist

Jeremy is the Technical Support Specialist and has been in his position since December 2023. He has a degree in Information Systems and experience in hardware and vulnerability management

2

What to Expect

Session Overview

Healthcare organizations face an unprecedented level of cyber threats. This session is designed to equip non-technical leaders with the knowledge they need to understand the rapidly evolving threat landscape and the critical security measures necessary to protect their organizations.

We will explore:

History of Hackers and Cybersecurity:
Understand the evolution of cyberattacks, from early hacking groups to modern-day threats, and how this shapes today's cybersecurity challenges in healthcare.

Understanding Hacker Motivations and Tactics:
Gain insights into why hackers target healthcare organizations and the strategies they use, including phishing, ransomware, and social engineering.

The Nature of Healthcare Cyber Threats:
Learn about the common threats facing healthcare, including ransomware, phishing, insider threats, and data breaches, and how these impact patient care and operations.

Essential Security Concepts:
Explore crucial security practices like Two-Factor Authentication (2FA) and encryption to help protect sensitive patient data and secure networks.

Practical Steps for Improving Security Posture:
Identify actionable measures non-tech leaders can implement to improve their organization's security, such as employee training, phishing simulations, and developing incident response plans.

This session provides non-tech leaders with a clear roadmap to effectively combat cyber threats in healthcare.

3

Bad Actors and Hackers

4

The Origin of the Term ‘Hacker’

The Origin of the Term 'Hacker'

1960s at MIT:

- The term "hacker" was first used at the Massachusetts Institute of Technology (MIT) in the 1960s.
- It originally referred to individuals who creatively explored and manipulated technology, particularly in MIT's Tech Model Railroad Club (TMRC) and later in the Artificial Intelligence (AI) lab.

Early Hackers:

- These early "hackers" were problem solvers who took pride in finding clever, innovative, and often playful solutions to complex problems.
- The term "hack" described a clever or unconventional solution, often done for fun or intellectual challenge.

Cultural Shift:

- The term "hacker" initially had no association with malicious activity; it celebrated technical expertise and curiosity.
- Over time, as computers became more accessible and hacking skills were applied to breaking into systems, the term began to take on its modern, often negative, connotation.

Hackers History and Timeline

Hacking has evolved over the decades, transitioning from the curiosity of early computer enthusiasts to a major cybersecurity concern with significant global implications.

1960s: The Birth of Hacking

- The term "hacker" was originally coined by MIT students who were exploring early computing systems and finding innovative ways to push the limits of technology. During this era, hacking was a term associated with problem-solving and creativity rather than illicit activity.

1980s: The Rise of Cybercrime

- With the personal computer boom in the 1980s, the hacking culture expanded, but so did the darker side of hacking. This period saw the first high-profile cases of cybercrime, such as the infamous 414s group who broke into government and corporate networks. The U.S. government responded by introducing the Computer Fraud and Abuse Act (CFAA) in 1986 to combat the growing number of cybercrimes.

1990s: The Formation of Hacking Groups

- The 1990s witnessed the emergence of notorious hacking groups like "Legion of Doom" and "Cult of the Dead Cow." These groups were responsible for numerous network intrusions, often battling with rival hacking groups. This period also saw the launch of DefCon, a major annual hacker convention that still runs today. Corporations and government agencies became frequent targets, and the rise of the internet opened the door for new vulnerabilities.

2000s: Financial Motives and Data Breaches

- As e-commerce and digital transactions became more widespread, hacking shifted from exploration to financial gain. Cybercriminals began targeting financial institutions, payment systems, and personal information for profit. Massive data breaches, such as the TJX hack in 2007, exposed millions of credit card details. At the same time, ethical hacking emerged as a profession, with companies hiring "white-hat" hackers to secure their systems.

2010s: The Dark Web and Nation-State Attacks

- In the 2010s, the Dark Web became a key marketplace for illegal activities, including the sale of stolen data, drugs, and weapons. Nation-state hacking also became a significant threat, as countries like Russia, China, and North Korea were accused of launching cyber-attacks for political and economic gain. High-profile attacks, such as the Sony Pictures hack in 2014 and the WannaCry ransomware attack in 2017, illustrated the growing global impact of cybercrime.

2020s and Beyond: The Future of Cybersecurity

- In recent years, hacking has become more sophisticated, with the advent of Artificial Intelligence and Machine Learning to automate attacks. Ransomware-as-a-service (RaaS) and cyber espionage continue to be critical threats. The focus has shifted towards securing the global infrastructure, including healthcare,

Hacker Groups Throughout the Ages

Historical Groups:

- **CDC (Cult of the Dead Cow):** Advocated for stronger cybersecurity, known for tools like "Back Orifice."
- **L0pht:** Shaped modern cybersecurity after testifying before Congress about internet vulnerabilities.
- **Legion of Doom (LOD):** Early hackers focused on telephone and network systems, rivaling the "Masters of Deception."

Modern Groups:

- **Anonymous:** Decentralized hacktivist group targeting governments and corporations.
- **APT28 (Fancy Bear):** Russian state-sponsored group involved in cyber-espionage.
- **REvil:** Ransomware-as-a-service group targeting healthcare and other industries.
- **ShinyHunters:** Responsible for high-profile data breaches, including AT&T and Microsoft.
- **Clop:** Launched ransomware attacks on organizations like Change Healthcare.
- **DarkSide:** Known for the Colonial Pipeline attack, focusing on critical infrastructure.

Modern Hacker Motivations, Jargon, and Types

Hacker Culture, Jargon, and Types of Hackers

•Motivations:

- **Financial Gain:** Hackers steal data or extort money.
- **Hacktivism:** Ideologically driven attacks.
- **State-Sponsored:** Targeting critical sectors for intelligence.

•Key Jargon:

- **Phishing:** Deceptive tactics for stealing credentials.
- **Zero-Day Exploit:** Exploiting unknown software flaws.
- **RAT (Remote Access Trojan):** Gaining remote access to systems.
- **Botnet:** A network of infected devices used in cyberattacks.

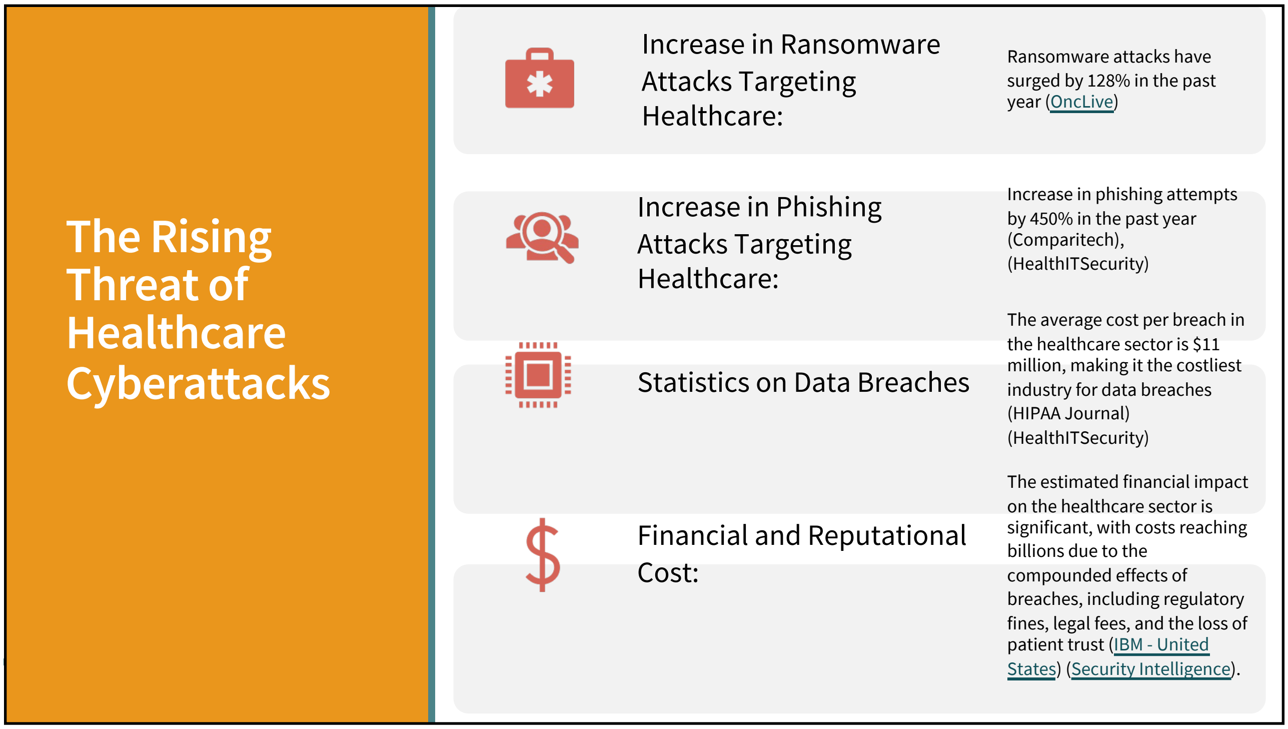
•Types of Hackers:

- **Black Hat:** Malicious hackers focused on financial gain or causing disruption.
- **White Hat:** Ethical hackers who help organizations improve their security.
- **Gray Hat:** Operate between legal and illegal actions, often without malicious intent.

Healthcare and Cyber Security

MN Community MEASUREMENT

9



The Rising Threat of Healthcare Cyberattacks

Increase in Ransomware Attacks Targeting Healthcare:

Ransomware attacks have surged by 128% in the past year (OncLive)

Increase in Phishing Attacks Targeting Healthcare:

Increase in phishing attempts by 450% in the past year (Comparitech), (HealthITSecurity)

Statistics on Data Breaches

The average cost per breach in the healthcare sector is $11 million, making it the costliest industry for data breaches (HIPAA Journal) (HealthITSecurity)

Financial and Reputational Cost:

The estimated financial impact on the healthcare sector is significant, with costs reaching billions due to the compounded effects of breaches, including regulatory fines, legal fees, and the loss of patient trust (IBM - United States) (Security Intelligence).

10

Common Cyber Threats in Healthcare

Malware (General Term):
- **Definition:** Broad term for any software designed to harm, including ransomware, viruses, Trojans, etc.

Ransomware:
- **Definition:** Malware that encrypts data and demands payment for release.
- **Example:** WannaCry, BlackCat

Viruses:
- **Definition:** Attaches to files and spreads when executed.
- **Example:** ILOVEYOU Virus.

Trojans:
- **Definition:** Disguised as legitimate software, providing backdoor access for loading of ransomware
- **Example:** Emotet, BO2k, Subzero

DDoS (Distributed Denial of Service):
- **Definition:** Floods a network or server with traffic, rendering it unavailable.
- **Impact on Healthcare:** Disrupts access to essential systems, like EHRs.

Advanced Persistent Threats (APTs):
- **Definition:** Long-term, targeted attacks, often state-sponsored.
- **Impact:** Infiltrates deeply into networks, often going undetected for months or years.

Why Bad Actors Target Healthcare Networks

High-Value Data:
- **Personal Health Information (PHI)** is extremely valuable on the dark web, often used for identity theft, insurance fraud, and selling prescription drugs.
- PHI includes sensitive details like social security numbers, medical history, and insurance data.

Outdated Systems:
- Healthcare providers often run legacy systems that lack modern security features and are difficult to patch.
- Many hospitals use a variety of connected medical devices (IoT) with weak security protocols.

Ransomware Potential:
- **Critical Operations**: Hospitals must stay operational 24/7, making them prime targets for ransomware attacks as downtime directly impacts patient care.
- **Higher Ransom Payments**: Healthcare providers are more likely to pay ransom quickly to restore services, fearing risks to patient safety and care delays.

Regulatory Pressure and Fines:
- Under HIPAA (Health Insurance Portability and Accountability Act), healthcare organizations face substantial penalties if patient data is compromised.
- The high cost of regulatory fines motivates hackers to target the sector, knowing that a breach can result in financial losses far beyond ransom payments.

Lack of Cybersecurity Investment:
- Healthcare organizations tend to underinvest in cybersecurity due to tight budgets focused on patient care.
- Cybersecurity staff shortages and limited training also contribute to the sector's vulnerability.

Patient Data and the Dark Web

Patient Data and the Dark Web

Healthcare data remains a lucrative target for cybercriminals due to its extensive details and high resale value on the Dark Web. Hackers exploit healthcare systems to steal sensitive medical information, which is then sold or exchanged in illegal markets. The comprehensive nature of patient data makes it highly attractive.

What Makes Patient Data Valuable:

Personal Identifiable Information (PII): Full names, social security numbers, and birthdates facilitate identity theft and fraud.

Medical History: Conditions, treatments, and prescriptions can be used for blackmail or fraudulent insurance claims.

Insurance and Financial Data: Hackers can submit false claims or exploit financial data for profit.

Additional Reasons Patient Data is Targeted:

Ease of Monetization: Stolen patient data provides multiple opportunities for hackers to profit through fraud, identity theft, and blackmail.

Shift to Telemedicine: As healthcare increasingly moves online, with telemedicine and remote services growing, new vulnerabilities arise in the systems used to deliver care, offering cybercriminals additional access points.

Black Market Demand: Medical records can be sold for high prices on illegal marketplaces, as they offer far more exploitable data than other forms of stolen information like credit card details.

THREATS TARGETING
CYBERCRIMINAL TAREATINGS PATIENT DATA
CYBERCRIMINAL THREATS PATIENT DATA
DARK W
DAICK
RK WEB TWORTS
DATA THUT

13

Why Most Breaches Are Not the Result of Advanced Cyberattacks

Failure to Implement Security Baselines:

A significant number of breaches are due to the lack of foundational security controls. Organizations often fail to implement basic defenses, such as multi-factor authentication (MFA), proper encryption, lack of patching, or routine access reviews.

Weak Password Policies: Many organizations still allow weak passwords or fail to enforce password complexity rules, making it easy for attackers to guess credentials.

Lack of Ongoing Monitoring and Incident Response:

Even when security baselines are implemented, they are often not monitored properly. This gives attackers an opportunity to exploit gaps for extended periods without detection.

Insufficient Logging and Alerts: Many breaches are not discovered for weeks or even months because there is no adequate monitoring in place. Breaches can go unnoticed due to the lack of real-time alerts on suspicious activities.

Human Error and Misconfigurations:

Misconfigured security settings or cloud environments are frequent causes of data breaches. Attackers can easily find misconfigurations and gain unauthorized access.

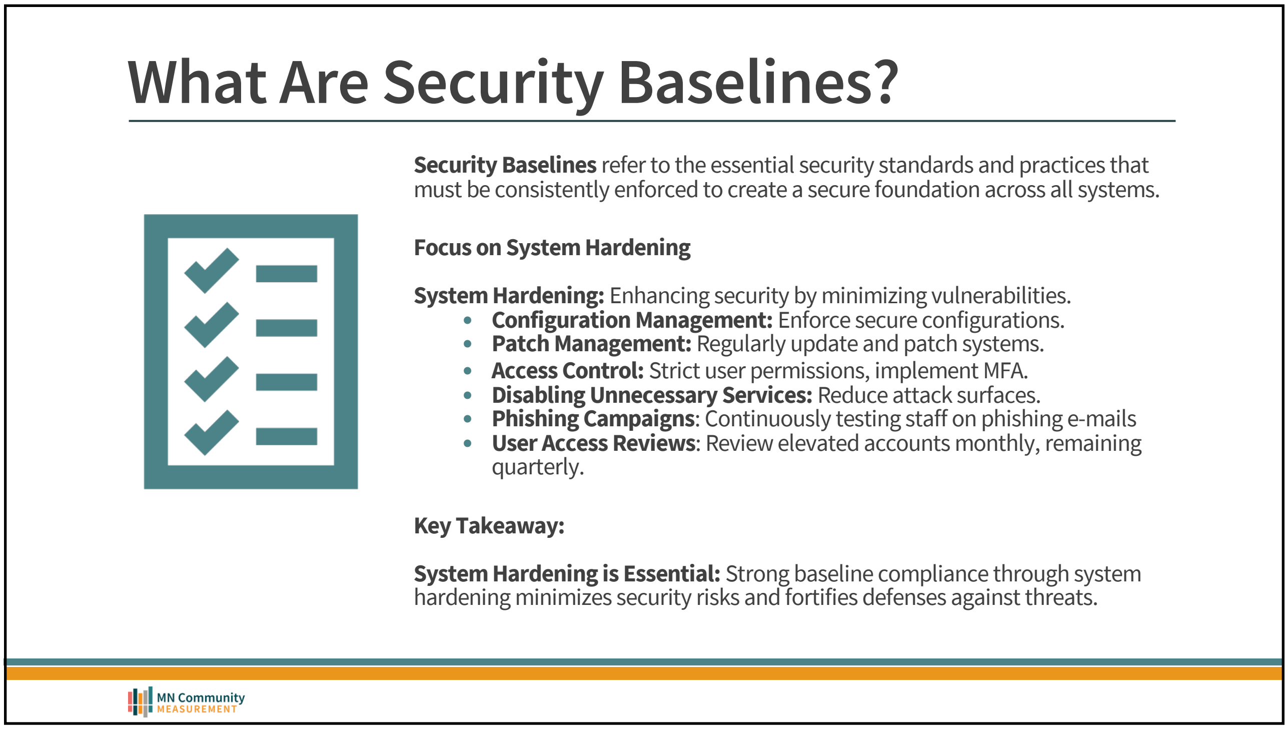
Insider Mistakes: Employees may unintentionally open phishing emails, share passwords, or misconfigure access controls, leading to security breaches.

Lack of a Security-First Culture:

Organizations that don't prioritize security in their everyday operations are more prone to breaches. Security must be integrated into every aspect of the business, not treated as an afterthought.

14

Avoiding Breaches by Implementing Baselines



What Are Security Baselines?

Security Baselines refer to the essential security standards and practices that must be consistently enforced to create a secure foundation across all systems.

Focus on System Hardening

System Hardening: Enhancing security by minimizing vulnerabilities.

- **Configuration Management:** Enforce secure configurations.
- **Patch Management:** Regularly update and patch systems.
- **Access Control:** Strict user permissions, implement MFA.
- **Disabling Unnecessary Services:** Reduce attack surfaces.
- **Phishing Campaigns**: Continuously testing staff on phishing e-mails
- **User Access Reviews**: Review elevated accounts monthly, remaining quarterly.

Key Takeaway:

System Hardening is Essential: Strong baseline compliance through system hardening minimizes security risks and fortifies defenses against threats.

Employee Training, Security Awareness, Phishing Campaigns

Continuous Security Training:

- Implement quarterly training sessions for all staff. MNCM utilizes a vendor for security and HIPAA training modules that includes mini-series productions to make security training entertaining while being informative for non-security staff.

Topics Covered in Training

- Recognizing and reporting phishing attempts.
- Best practices for password creation and management.
- Secure handling and sharing of sensitive data and hundreds of others

Phishing Campaigns

- Organizations should regularly conduct phishing campaigns against staff to test training received.
- If a staff member fails a phishing test, they should be automatically enrolled in security training.
- Implement an e-mail headers if senders e-mail originated outside of the network

Multi-Factor Authentication (MFA) – System Hardening

Why Multi-Factor Authentication (MFA)?

- MFA is a crucial step in system hardening, adding an extra layer of security by requiring multiple forms of verification before granting access. This significantly reduces the risk of unauthorized access, even if a password is compromised. This feature is often looked today as being legacy or old tech, in favor of more complex security.
- Microsoft stated in 2022 that 92% of all Office breaches would have been avoided if customers had turned on MFA. (Now being required by Microsoft beginning October 15, 2024)

Require MFA on All Organizational Systems & Vendors

- Require that MFA is on for all internal systems (Office 365, Github, Slack, EHR, E-mail, etc.)
- Require by Security Assessment that all your vendors implement MFA on systems that are utilized by your organization

System Hardening is Critical: Importance of MFA

MFA Could Have Prevented Many Recent Data Breaches: A significant number of recent high-profile data breaches occurred due to the lack of Multi-Factor Authentication (MFA). Attackers gained unauthorized access through compromised credentials, exploiting weak single-factor authentication methods.

Adding a Layer of Security: MFA requires users to verify their identity through two or more factors (e.g., a password and a mobile verification code), significantly reducing the risk of unauthorized access.

Proven to Stop Attacks: Implementing MFA could have prevented many of these breaches by blocking attackers even if they had obtained valid credentials.

Low Hanging Fruit: Rather than attempting sophisticated attacks, these bad actors often target the simplest weaknesses, such as systems lacking Multi-Factor Authentication (MFA) or those with weak passwords. These low-effort attacks can lead to significant breaches if basic security measures are not in place.

Missing Baselines: Baselines that are unproven are not reliable. Organizations must test their security baselines often to ensure validity of baseline.

19

Lessons in Baseline Compliance

Equifax (2017)

How it happened: Equifax, a major credit reporting agency, was hacked due to its failure to apply a security patch for a known vulnerability in its Apache Struts web application framework. This failure to follow basic patch management practices exposed sensitive personal data of 147 million people, including social security numbers.

Key baseline issue: Lack of patch management and failure to monitor vulnerabilities.

Colonial Pipeline (2021)

How it happened: Colonial Pipeline, the largest fuel pipeline in the U.S., was breached in 2021 through a compromised password that lacked multi-factor authentication. Hackers used a leaked VPN credential to gain unauthorized access to the pipeline's systems. The password had been exposed in a previous data breach, but the absence of MFA allowed attackers to exploit it.

Key baseline issue: The use of single-factor authentication (just a password) allowed hackers to gain access using a compromised credential.

AT&T and Snowflake (2024)

How it happened: AT&T experienced a significant breach tied to Snowflake, its cloud service provider. Hackers exploited accounts that lacked **multi-factor authentication (MFA)**, allowing them to steal call logs of nearly 110 million customers. Though sensitive information like Social Security numbers was not included, the stolen metadata provided enough details for attackers to conduct targeted attacks, identity theft, and other malicious activities.

Key baseline issue: The lack of enforced MFA for customer accounts using Snowflake, which relied on single-factor authentication, made it easier for hackers to access data.

20

Key Takeaways

Understanding Bad Actors and Hackers

Hackers are motivated by various goals, including financial gain, hacktivism, and state-sponsored espionage.

Familiarity with hacker culture, key terms like phishing and zero-day exploits, and knowledge of famous hacker groups is essential for preparing effective defense strategies.

Rising Cyber Threats in Healthcare

The healthcare sector faces growing risks from ransomware, phishing, and other malware attacks, with a significant increase in both frequency and sophistication.

Patient data is highly valuable on the Dark Web, making healthcare organizations prime targets for cybercriminals.

Importance of Security Baselines

Implementing strong security baselines, such as multi-factor authentication (MFA), encryption, and regular patching, is critical in protecting healthcare systems.

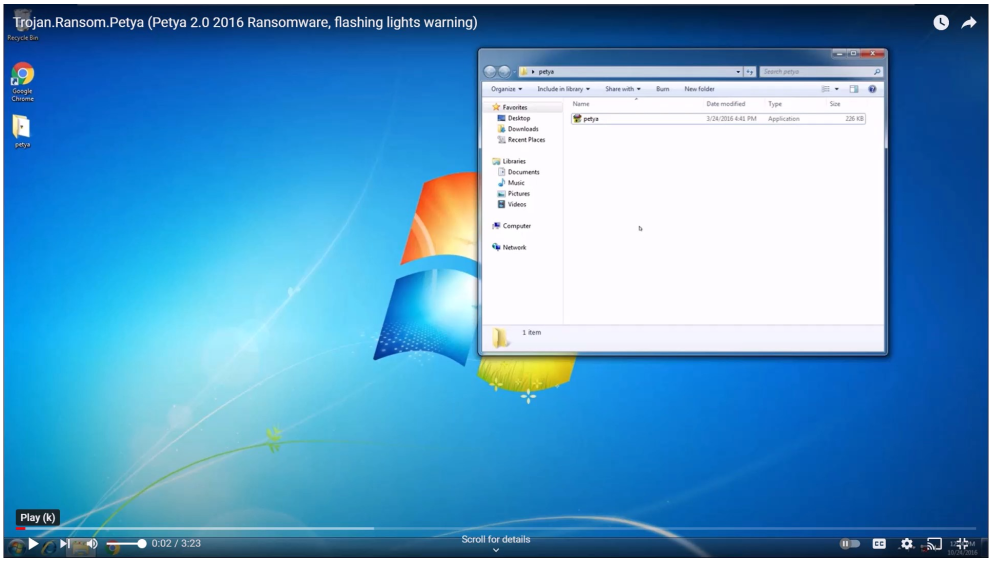
A Zero Trust model ensures that all access requests are verified, reducing the risk of unauthorized breaches.

Mitigating Cyber Risks

Regular employee training, phishing campaigns, and security validation tests can significantly reduce the likelihood of successful cyberattacks.

Demonstrations of real-world ransomware attacks highlight the importance of proactive security measures.

21


Trojan.Ransom.Petya (Petya 2.0 2016 Ransomware, flashing lights warning)

22