
Navigating Cyber Threats
Practical Steps to Protect Your Business and Personal Lives
nekey
nekey.com | 888-869-1331

INTRO / STORY

In the recent cybersecurity presentation, we explored one of the most consequential cyber incidents in recent history. This case, while based on the high-profile breach that halted operations at a major infrastructure organization, serves as a stark reminder of the vulnerabilities inherent in today's digital landscape. The incident unraveled when an employee received a ransomware popup on their workstation. Swiftly reporting it, the employee set off a chain of events that led to the full shutdown of the organization's operational structure, escalating all the way to congressional attention and even triggering a national emergency declaration.

At the heart of the breach was an unmonitored point of entry: the employee's VPN access. The employee, who had been working remotely, had left the organization over a year before the incident, but their VPN access remained active, and the password hadn't been reset. Although this was not a simple password—complex in nature and intended to be secure—it had been leaked in a large-scale dark web credential dump known as "RockYou2021." This dump, which included over 8 billion compromised credentials from various platforms, demonstrated the far-reaching consequences of password reuse and password theft. Even robust passwords aren't immune when they appear in repositories that cybercriminals frequently use for attacks.

The compromised password was likely obtained through one of two methods: phishing, where the employee may have unknowingly provided login information on a fraudulent website, or password reuse, wherein the same password was applied to multiple accounts, one of which may have been previously compromised. The attackers employed a password spray technique, trying the leaked credential on various accounts within the organization, eventually gaining unauthorized access. Unfortunately, despite the complex password, the absence of two-factor authentication (2FA) on the VPN connection removed the critical layer of protection that could have thwarted this access attempt.

While this story revolves around a major organization, it serves as a critical lesson for small businesses as well. In fact, small businesses are even more vulnerable to these types of attacks, as they often lack the resources and layered defenses of larger corporations. When high-profile breaches affect large enterprises, they make headlines; but for many small businesses, a single cyber incident of this nature can lead to irreversible consequences, including the potential for closing their doors entirely.

These incidents may never make the news, but the reality is that cybercriminals frequently target smaller organizations, exploiting similar gaps in security with devastating effect. Without the proactive defenses and response plans that larger entities typically have in place, small businesses face increased risk of severe operational and financial damage. That's why we focus on delivering comprehensive, scalable cybersecurity solutions designed to protect businesses of all sizes from these very real, very preventable threats. A proactive approach, from basic safeguards to advanced monitoring, is crucial in today's landscape—not just to prevent breaches, but to ensure business continuity and resilience.

©neKey, 2024

Key Cybersecurity Principles for Businesses and Individuals

During the presentation, we explored several crucial aspects of cybersecurity, some of which were highlighted in the story of that major cyber incident. These principles are essential for businesses of any size, as well as for personal cybersecurity habits. Each point represents a practical step toward building a resilient cybersecurity posture that can help mitigate the risk of similar incidents.

1. **Implement Modern Detection and Response Systems**
   - Having advanced detection and response capabilities enables early identification of potential threats. These systems can alert security teams to unusual activities, allowing for a swift and effective response.
2. **Keep Operating Systems and Software Up-to-Date**
   - Cybercriminals often exploit vulnerabilities in outdated or unpatched software. Regular updates and security patches help close these gaps, minimizing the risk of exploitation.
3. **Avoid Reusing Passwords Across Accounts**
   - Reusing passwords increases vulnerability, as credentials leaked in a breach can grant unauthorized access to multiple accounts. Using unique passwords for each account is essential to prevent this risk.
4. **Maintain a Robust Backup and Recovery Strategy**
   - Reliable backup solutions ensure data can be quickly restored in the event of an attack or other disruptions. Regular, secure backups stored off-network are critical to minimizing downtime and data loss.
5. **Establish Strong Internal IT Procedures**
   - Effective account management is vital, including timely disabling of former employees' access and regular password updates. Well-defined IT procedures help ensure that only active, trusted users have access to critical systems.
6. **Enable Multi-Factor Authentication (MFA)**
   - Adding MFA to login processes strengthens security by requiring a second form of verification, such as a code or biometric check, along with a password. This extra layer significantly reduces unauthorized access risks.
7. **Provide Ongoing Cybersecurity Awareness Training**
   - Regular training helps employees and users recognize phishing attempts and other cyber threats. Educating staff on security best practices reduces the likelihood of falling victim to common attacks.
8. **Use Encryption to Protect Devices from Theft and Loss**
   - Encryption protects sensitive information on devices, ensuring that data remains secure even if a device is lost or stolen. This is especially important for laptops, tablets, and mobile phones used in remote work.
9. **Protect Cloud and SaaS Environments with Monitoring**
   - As businesses increasingly rely on cloud services and Software-as-a-Service (SaaS) platforms, securing these environments from unauthorized access is essential. Continuous monitoring and secure configurations help safeguard data in the cloud.
10. **Monitor the Dark Web for Compromised Credentials**
    - Dark web monitoring services can alert you if your credentials appear in data dumps on illicit marketplaces, allowing you to take swift action to change passwords and secure accounts. This proactive approach minimizes the risk of threat actors gaining unauthorized access through leaked information.
11. **Stay Vigilant Against Social Engineering Attacks**
    - Always question the legitimacy of codes sent via text, unexpected emails, and even calls claiming to be from familiar institutions. Malicious actors can easily spoof phone numbers, email addresses, and SMS senders. Being cautious and verifying the source can prevent phishing, vishing, and smishing attacks that exploit trust to gain access.
12. **Partner with a Managed Service Provider (MSP) for Comprehensive Cybersecurity**
    - Engaging an MSP provides businesses with expert management of cybersecurity tasks, from threat monitoring to incident response. An MSP can deliver the layered protection that is essential in today's complex threat landscape, helping businesses stay secure without requiring extensive in-house expertise.

By following these principles, businesses and individuals alike can strengthen their defenses against cyber threats. These guidelines not only address the specific vulnerabilities seen in major incidents but also promote proactive cybersecurity habits that can prevent breaches and maintain resilience across all levels.

©neKey, 2024

1 Implementing Next-Gen Antivirus (AV) and Endpoint Detection & Response (EDR)

Traditional antivirus programs are now largely obsolete in today's complex threat landscape. Modern cyber defense requires more than blocking known viruses; it must combat sophisticated, emerging threats designed to infiltrate systems, remain hidden, steal data, and deploy ransomware. Next-gen antivirus (AV) systems leverage advanced algorithms, machine learning, and behavioral analysis to detect suspicious activity before damage occurs. When combined with Endpoint Detection and Response (EDR), these tools provide real-time monitoring, detection, and response, creating a robust defense against sophisticated attacks and ensuring businesses stay protected in an ever-evolving cyber landscape.

For Business

- **Stop using traditional, old technology antivirus.**
- **Look into a managed Next-Gen AV (EDR) solution.**
- **Augment your Next-Gen AV (EDR) with a SOC or MDR (managed detection and response).**

For Personal

- **Use products from companies that provide EDR on the business side. They reuse some of the technology for home products.**
- **Ensure your subscription is always up to date.**
- **Periodically evaluate your vendor by reviewing independent tests such as AV Comparatives.**

SentinelOne CROWDSTRIKE deepinstinct BEFORE YOU KNOW IT Bitdefender eset Malwarebytes

2 Keeping Operating Systems and Software Up-to-Date

Keeping operating systems and software consistently updated is one of the simplest yet most effective cybersecurity measures. Cybercriminals often exploit known vulnerabilities in outdated software to gain access to systems. Regular updates and patches close these security gaps across all devices and applications, significantly reducing the risk of exploitation and maintaining a more secure digital environment for both businesses and individuals.

Zero-day vulnerabilities—security flaws unknown to the software vendor—are especially dangerous, as they allow attackers to bypass standard defenses. Installing urgent patches is critical, as they often address weaponized zero-day threats, providing timely protection against active exploits. Regular updates reduce the number of known vulnerabilities, while tools that detect abnormal behavior offer additional defense against these hidden threats.

For Business

- **Have a process or a vendor that enforces updates. Don't assume they get automatically installed and are successful without oversight.**
- **Extend that process to 3rd party products. It is not just Windows, it is not just Mac OS, you have to update third party applications too. Adobe, Autodesk, all of them contain critical vulnerabilities.**
- **Consider a Vulnerability Scanner solution.You can implement a network scanning service that looks at all of your devices and lets you know if something is vulnerable and updates are missing.**

For Personal

- **Keep your home computer up to date. Restart your computer when asked, and restart it in general, it keeps your update stack healthy.**
- **Patch vendor firmware and drivers too. Use vendor utility on your PC (DELL, Lenovo, HP).**
- **If you are on a Mac, do not assume it is bulletproof. Mac malware is out there, update frequently and do not use your old Mac if it is no longer supported by latest Mac OS.**

©neKey, 2024

3 Avoid Reusing Passwords Across Accounts

Password reuse is a risky practice that can lead to breaches across multiple accounts if one platform is compromised. Cybercriminals exploit this through “password spray” attacks, where leaked credentials are used to access unrelated systems. Using unique passwords for each account is crucial for security.

Password management apps simplify this process by generating, storing, and encrypting complex passwords. They allow both businesses and individuals to maintain strong password hygiene, reducing the risk of password-related attacks. For businesses, they also streamline secure credential sharing, while for individuals, they offer convenience without compromising security.

For Business

- **Sign up for business edition of password manager apps.**
- **Establish and enforce internal procedures to store all company passwords in a password manager.**
- **Audit your network and cloud and remove Excel spreadsheets with passwords.**

For Personal

- **Get into the habit of making a new random password for every account you sign up for. Store them in the password manager.**
- **Revisit old accounts that are using your favorite common password, change to secure one.**
- **Ensure you have a backup of your password manager on more than one device.**

1Password DASHLANE bitwarden

4 Maintaining a Robust Backup and Recovery Strategy

Backups are the last line of defense in cybersecurity, ensuring that critical data and systems can be restored after an incident. However, for backups to be effective, they must be Healthy, Recent, and Verifiably Operational.

A healthy backup is free from corruption, recent backups minimize data loss, and verifiably operational backups are tested regularly to ensure they can be restored when needed. By following these principles, businesses can rely on their backups as a dependable safeguard, reducing operational disruption and data loss in case of a cyber incident.

For Business

- **Use 3-2-1 backup strategy:**
  (1) production data
  (2) isolated onsite copy
  (3) offsite cloud copy.Design network to separate backup servers from your primary LAN. Don’t assume cloud backup is 100% safe. Never keep all of your eggs in one basket.
- **Ensure backup data is encrypted, at rest and in transit. Protect backup console with password. Test recovery and test all operations.**
- **Consider immutable (WORM) backup, where cloud data cannot be changed or modified once uploaded. Invest into BCDR appliance for rapid onsite recovery.**

For Personal

- **Use backup service like Carbonite to backup all of your computer data automatically.**
- **Consider Microsoft OneDrive, it will redirect your Documents and Desktop and serve as backup for them.**
- **Use iCloud on your Mac to backup your data, invest into additional storage. Check your backups! Even on iPhones it is not set it and forget it.**

©neKey, 2024

5 Establishing Strong Internal IT Procedures

Strong internal IT procedures are vital for cybersecurity, ensuring only authorized users access sensitive systems. Key practices include managing user access, promptly disabling former employees' accounts, updating passwords, and auditing permissions regularly. Without structured IT protocols, organizations risk insider threats and unauthorized access.

Comprehensive documentation is equally essential. Detailed records of IT procedures, system configurations, and access controls prevent knowledge gaps if an employee leaves, the IT person departs, or the IT vendor goes out of business. Proper documentation ensures continuity, allowing new personnel or vendors to manage and secure systems effectively without missing critical information.

Asset Management and Procedure Documentation

- **One of the pillars of cybersecurity is documentation and audit of all assets, both hardware and software. Documented IT = Successful IT.**
- **You can use your password manager to securely store any documents, spreadsheets, PDFs, and images, and of course, account information.**
- **Asset Documentation is not very useful if there are no procedures – remember the domino of still active account? Your Backup Process - is it documented and easily accessible when disaster strikes?**
- **Procedures are great but they also must be enforced, audited, and followed by all. Ask your IT vendor for their documentation.**

6 Enabling Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) adds a critical layer of security by requiring users to verify their identity with a second method beyond a password, such as a one-time code or biometric check. This makes unauthorized access much harder, especially against attacks like password spray.

Authenticator apps, like Google Authenticator or Authy, offer more secure alternatives to SMS-based codes, which are vulnerable to SIM swap attacks. However, vigilance is still necessary, as cybercriminals use tactics like 2FA phishing to steal codes. Combining MFA with user awareness and training enhances security and maximizes protection against unauthorized access.

For Business

- **Adopt 2FA everywhere strategy.Start with email accounts, evaluate remote access and VPN, and have a policy that automatically enforces 2FA for all users.**
- **Ensure that all administrator accounts are always 2FA protected. Don't forget about Office365 admin access (or Google Workspace Super Admin).**
- **Always have a secondary recovery or login method. Create two global admins, both protected with 2FA, and ensure your IT vendor is set up as partner or admin relationship.**

For Personal

- **Choose a reputable Authenticator App vendor. Ensure that the data is encrypted, protected, and backed up, whether in the cloud, phone backup, or secondary device that you own.**
- **Go through all your accounts and services. Switch to Authenticator-based 2FA where possible. Account -> Profile -> Security**
- **Remain vigilant. Do not automatically trust a 2FA prompt, text message, or phone call asking for a code sent to your device.**

©neKey, 2024

7 Providing Ongoing Cybersecurity Awareness Training

Cybersecurity awareness training is essential for building a security-conscious culture. Employees, often the first line of defense, need regular training to recognize threats like phishing emails, suspicious links, and social engineering tactics. Practical, scenario-based training helps them understand what to look for and how to report suspicious activity.

Phishing simulations further enhance training by safely testing employees' ability to detect scams. These exercises identify areas for improvement and reinforce good cybersecurity habits. Ongoing training and simulations help reduce successful attacks, as employees become better at spotting potential threats before they escalate. Effective cybersecurity training is an evolving, continuous process.

For Business

- **Establish a recurring, regular cyber awareness training course for everyone in your organization.**
- **Couple this recurring cyber awareness training with ongoing phishing simulation campaigns.**
- **Review reports and address gaps in training, sign up for new courses that cover new phishing techniques, and educate users that got test phished.**

For Personal

- **Take free cyber security awareness training course from Amazon. Yes, Amazon!** *https://learnsecurity.amazon.com*
- **Check out free videos on YouTube.**
- **You can't be certain who sent that SMS.**
  You can't be certain who called you.
  You can't be certain who emailed you.

KnowBe4.com Human error. Conquered. | ID AGENT | BREACH SECURE NOW

8 Using Encryption to Protect Devices from Theft and Loss

Encryption is essential for protecting sensitive information on both personal and business devices, making data inaccessible without the decryption key if a device is lost or stolen. Applying encryption to laptops, mobile devices, and storage drives ensures that data remains safe from unauthorized access.

For businesses, encryption is crucial for regulatory compliance and data breach prevention, while on a personal level, it secures financial and private information. Full-disk encryption is recommended, as it protects all data on a device rather than just individual files. Encryption provides a robust layer of security, safeguarding data even if physical security fails.

For Business

- **Enable BitLocker drive encryption on all computers and servers.**
- **Make sure the encryption is centrally managed by a vendor or cloud solution, like Microsoft 365.**
- **Have a policy and procedure in place to ensure device and data encryption is consistent. There is nothing worse than not being able to access your own information.**

For Personal

- **Lookup on how to enable BitLocker on your computer.**
- **Make sure you document BitLocker key well:**
  (1) printed copy
  (2) store it in the password manager
- **Sleep well knowing you can even dispose of old computer that has been encrypted (if it has a TPM chip).**

©neKey, 2024

9 Protecting Cloud and SaaS Environments with Monitoring

Securing cloud and SaaS environments demands constant vigilance, as they often contain sensitive data and essential business processes. Monitoring unusual activity, like excessive file deletions or access from unexpected locations, can help detect security threats early. Regularly auditing accounts, especially those of former employees, ensures that only authorized users have access. By actively managing permissions and responding to suspicious behavior, businesses can better protect their cloud data from unauthorized access and accidental exposure.

Cover your SaaS!

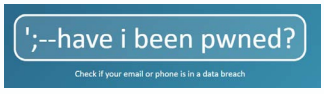
- **Who is watching your cloud? What if someone logs in from another country? Or deletes many files at once?**
- **Are you promptly disabling users when they leave your firm?**
- **If you put everything into the cloud, make sure it has a backup, cloud to another cloud.**
- **Ensure that all activity in your cloud is monitored and suspicious events are reviewed by a vendor or partner.**

10 Monitoring the Dark Web for Compromised Credentials

Monitoring the dark web for compromised credentials is a proactive step every business should take to protect sensitive information. Through their IT provider or cybersecurity partner, businesses can keep an eye on their domain to detect if employee or client data appears on the dark web, allowing them to take swift action if a breach is discovered. For individuals, resources like Have I Been Pwned offer a safe and trustworthy way to check if personal email accounts have been compromised in past data breaches. By staying informed of potential leaks, both businesses and individuals can promptly update passwords and strengthen security to reduce the risk of unauthorized access.

Darkweb Monitoring

- **See if your credentials popup on Dark Web (in RockYou2021)**
- **Set up the service for your business to monitor your domain and get notified**
- **For personal protection, use *haveibeenpwned.com***
- **Input all of your emails in there to get notifications if they were in a breach**
- **Check all your common passwords against the service**
- **Yes, it is safe and reputable – you are not giving your passwords away**



©neKey, 2024

11 Staying Vigilant Against Social Engineering Attacks

Social engineering attacks, like phishing, vishing, and smishing, manipulate individuals into revealing sensitive information. To stay safe, approach unexpected emails, texts, or calls with caution—even if they appear to be from trusted sources, as attackers can spoof these. Always verify requests for sensitive information and maintain a mindset of skepticism. Vigilance helps users avoid falling victim to these increasingly sophisticated tactics.

And remember, in today's digital landscape, a little paranoia goes a long way:

- **"You can't be certain who sent that SMS.**
- **You can't be certain who called you.**
- **You can't be certain who emailed you."**

Approach each interaction with caution, and always verify the identity of the sender or caller before sharing any information. In cybersecurity, trust should be earned, not assumed.

12 Partnering with a Managed Service Provider (MSP) for Comprehensive Cybersecurity

In today's complex threat landscape, partnering with a Managed Service Provider (MSP) offers businesses robust cybersecurity without the need for in-house expertise. MSPs provide end-to-end security services—monitoring, threat detection, incident response, and proactive maintenance—tailored to protect business data and systems. By leveraging a team of experts who stay current on the latest threats and best practices, businesses ensure comprehensive, up-to-date cybersecurity.

For smaller organizations, an MSP offers enterprise-level security affordably, making advanced protection accessible and scalable. MSPs also manage essential security protocols like backups, encryption, and monitoring, allowing businesses to focus on core operations, knowing their cybersecurity is managed by professionals dedicated to their safety.

For Business

- **Cybersecurity will keep you savvy with your data, privacy, and keeping safe things we take for granted.**

For Personal

- **Cybersecurity will futureproof your business, and it will make you more competitive.**

©neKey, 2024

Contact neKey today to learn more about our Cyber Security and comprehensive Managed IT Solutions.

nekey

nekey.com | 888-869-1331