Ransomware 2.0
Prevention is Your Best Option

NPC Safe Computing Webinar Series

February 14th, 2023

Larry Keating, President
Darren Mar, National Sales Manager

NPC DataGuard™

Presenters

Larry Keating
President

30+ years' experience with information technology, remote communications and data security.

Darren Mar
National Sales Manager

10+ years in SMB technology products and services, with emphasis on financial services small office security.

Thank You!


ALIGNED
capital partners inc.


Serenia Life
FINANCIAL


HUB


PPI


TruStone
financial


SIDEDRAWER™


Advocis
The Financial Advisors
Association of Canada


MANDEVILLE
PRIVATE CLIENT INC.


EQUITY
Associates Inc.


Carte
WEALTH MANAGEMENT INC.
RISK MANAGEMENT INC.


AON


Manulife Securities


GROVE POINT
FINANCIAL


Investment
Planning Counsel®
IPC VALEURS MOBILIÈRES


HollisWealth


IDC
WORLDSOURCE
INSURANCE NETWORK INC.


Advisor
Research
Group Inc.


CI FINANCIAL


IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES


FINANCIAL LITERACY
COUNSEL INC.


GLOBAL
MAXFIN INVESTMENTS INC.

NPC Solutions

Secure managed computers and Microsoft 365 for the professional and SMB office.

- NPC Secure Managed Computers
  - Hardware, encryption, backup, system software, security, technical support, managed and monitored for you
- NPC Managed Microsoft 365
  - SharePoint, Exchange Email, Teams, and a host of productivity tools
- Dedicated Account Manager
  - A custom and consultative approach

Agenda

- What is Ransomware?
- Current Threats & Impacts
- What to Do

What is Ransomware?

Ransomware

Definition:

Malicious software, referred to as malware or a virus, that blocks access to files, applications, or the use of a computer through encryption or taking control of the computer until a ransom is paid.

Designed to achieve:

- Operational Disruption
- Extortion
- Data Theft

Attack Methods

Threats are up

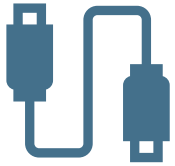
300%

since the pandemic started

Source: FBI IC3 (Internet Crime Complaint Centre)

Phishing emails and web browsing

Remote desktop

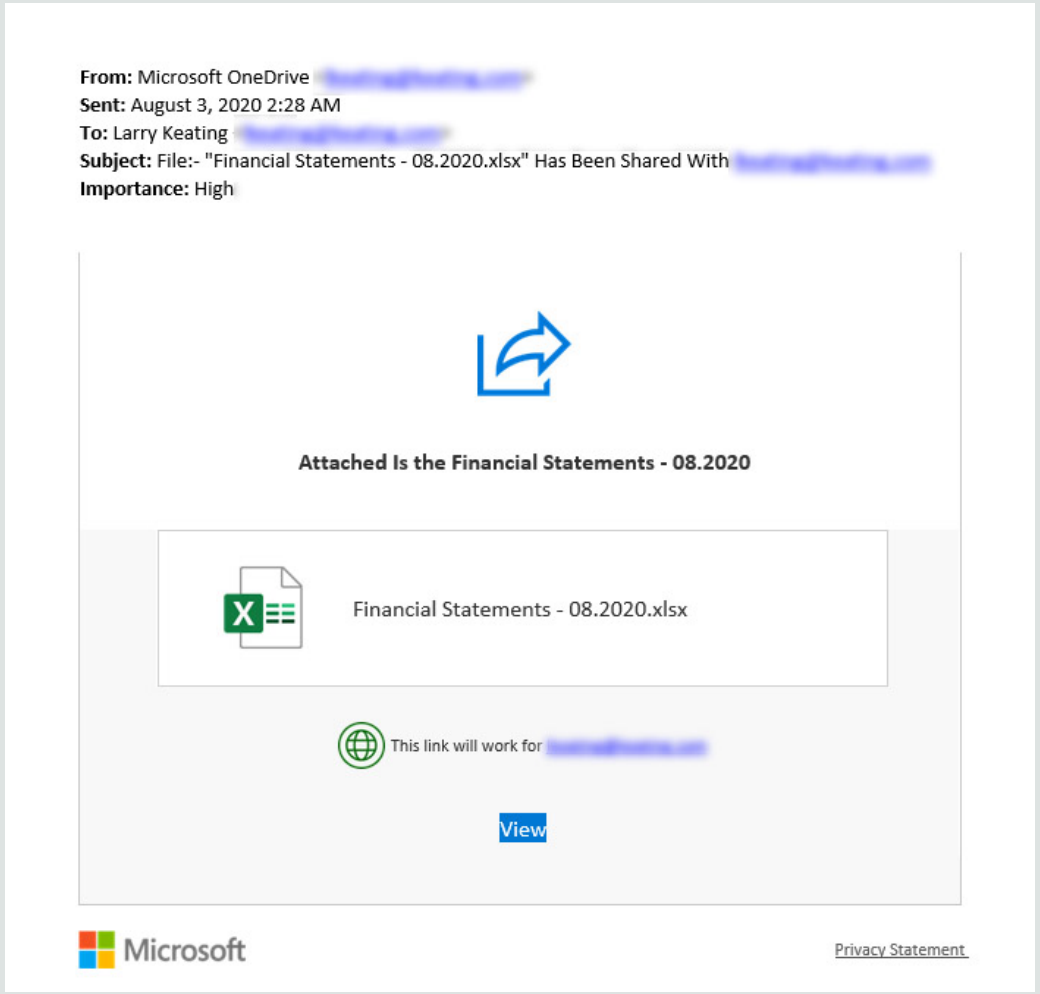


Improperly Protected Networks

IoT devices

Supply Chain Attacks

Familiar Business Look



From: Microsoft OneDrive [redacted]
Sent: August 3, 2020 2:28 AM
To: Larry Keating [redacted]
Subject: File:- "Financial Statements - 08.2020.xlsx" Has Been Shared With [redacted]
Importance: High

Attached Is the Financial Statements - 08.2020

Financial Statements - 08.2020.xlsx

This link will work for [redacted]

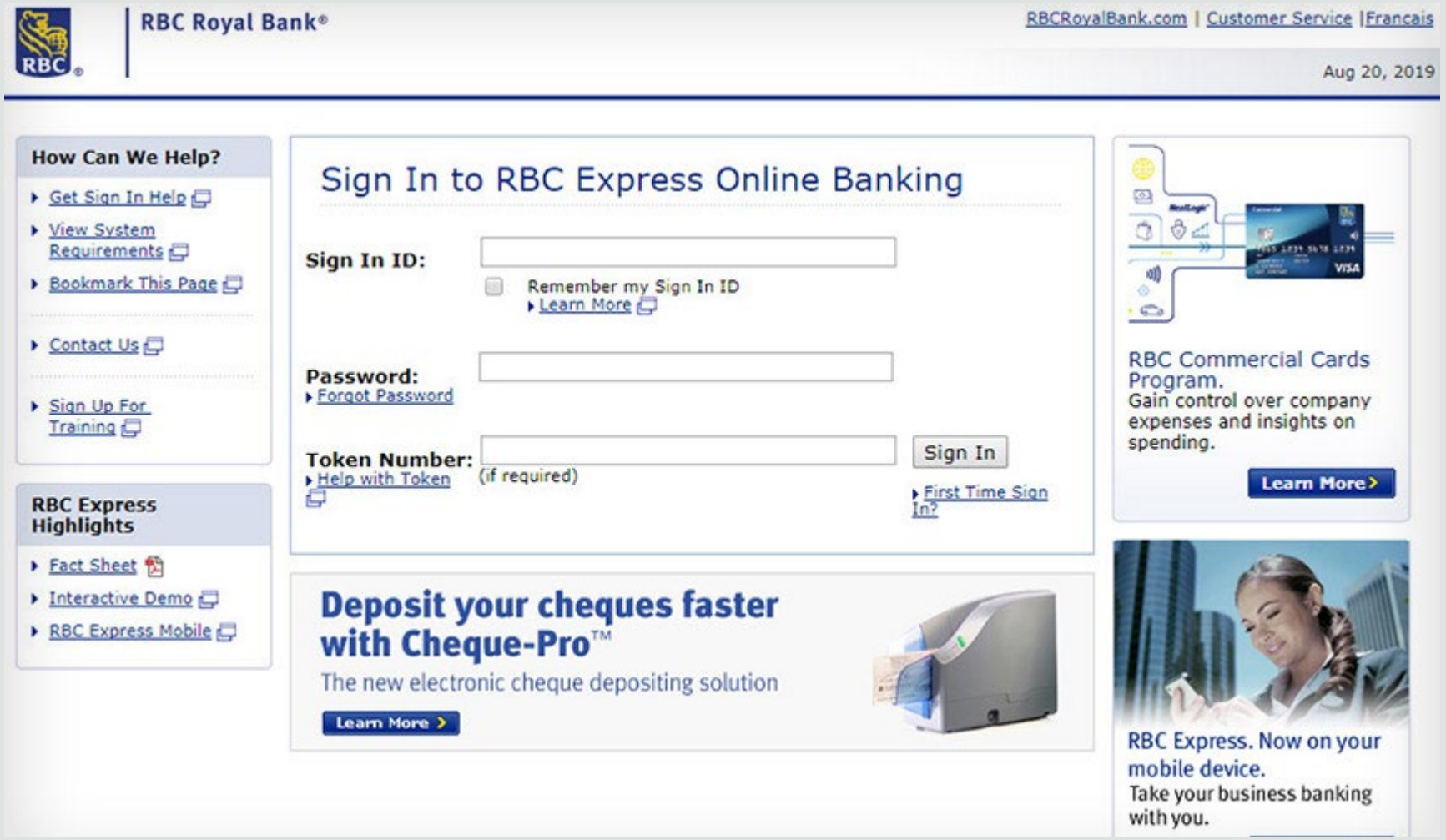
View

Microsoft

Privacy Statement

Source: NPC Files

Spoof Banking Website



Tactics to Coerce Payment

Encryption:

- The most common tactic, makes it impossible to access your files

Lockers:

- Blocks your access to your computer, network or applications

Scareware:

- Coercing victims into buying unnecessary software or services, including unrelenting pop-ups, intermittent access restrictions and disrupted computer performance

12

Increase in Tactics to Coerce Payment

Doxing:

- Steal and leak data if ransom to unlock not paid
- May cause violation of contract terms, non-disclosure agreements, privacy laws, securities laws, loss of intellectual property, or intellectual property protection

Shaming:

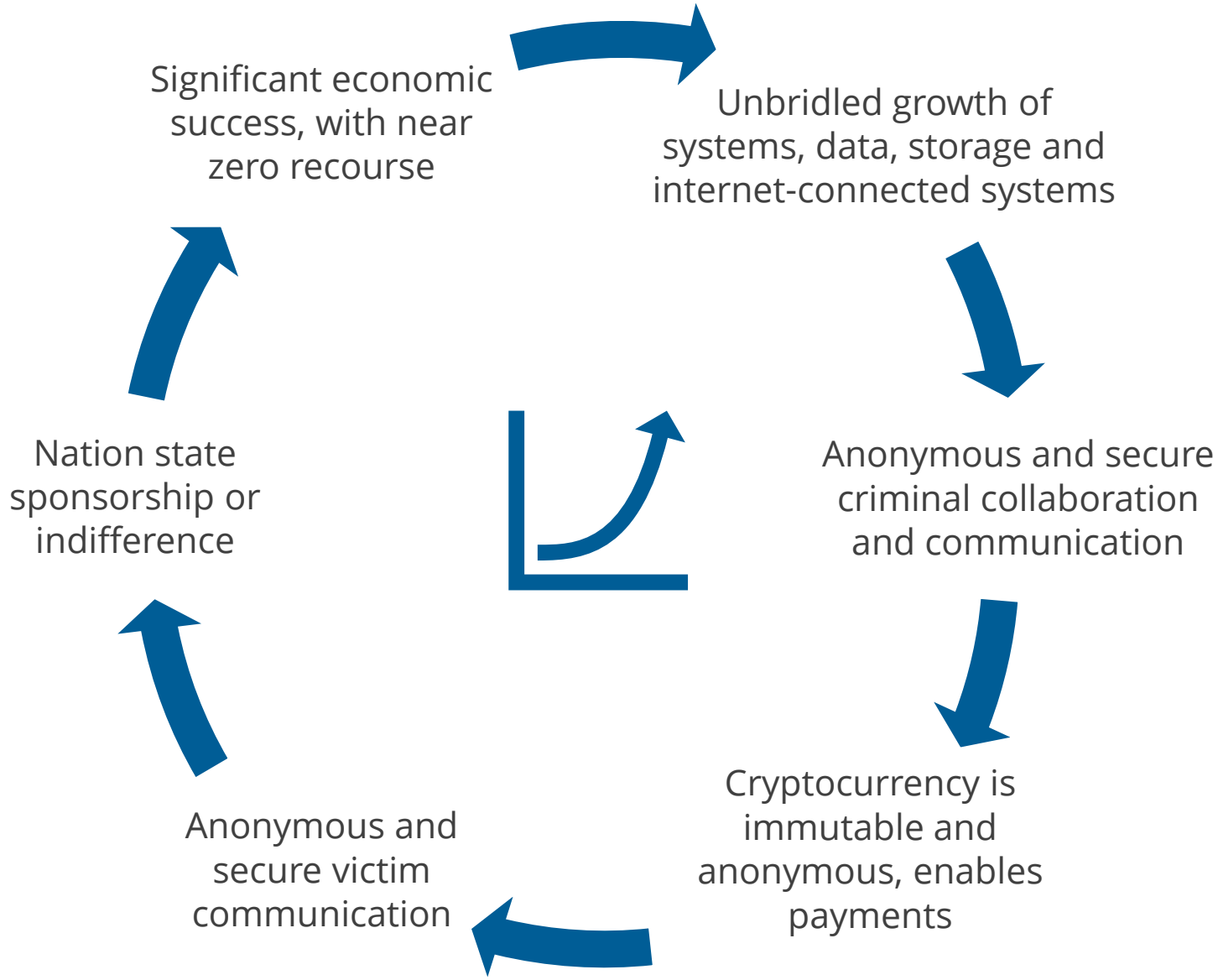
- If ransom still not paid, advise victim's clients, suppliers, partners, etc., of the breach via victim's social media and stolen email lists

Double-Encrypting:

- A second layer of encryption requiring a different key, or two or more segments of data have different keys

13

Why is it Growing?



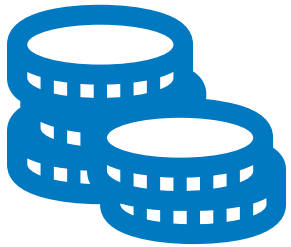
Source: NPC Files

Current Impacts

What's the issue in 2023?

Ransomware is now the leading form of cyber attack causing massive business disruption and losses

Attacks are increasing in effectiveness



Higher costs and business impacts

All business sizes a target

Small business is the target…

Sources: Forbes Magazine July 27,2021 | Tech.co, February 7, 2022 | BC Business, July 2022

Attacks are becoming increasingly complex, effective and costly

- Criminal factions behind them are more organized, more “professional”
- Ransoms for even single-person offices can be $10,000 - $100,000, or up to millions for larger entities
- Remediation costs are up as the criminals use technology to attack connected computers, backups, and even cloud storage
- Brand and financial damage from an attack can be considerable

Concerns for professional services

- Professionals are top targets, extra vigilance required
- Blended Attacks combining cyber attack and traditional financial crime are emerging:
  - e.g., before ransomware lock-up, steal client personal information to create money laundering accounts
- Mandatory reporting of client information loss the norm for regulated professionals

Why not just pay the ransom?

It is technically unnecessary:

- The technologies exist to seamlessly back up servers, endpoint computers, even the attached smartphones, economically and reliably
- Layers of defense thwart most attacks. 91% of successful malware penetrations are “known signatures” or the result of unpatched systems
- Decryption keys do not always work
- Prevention is cheaper than remediation

Why not just pay the ransom?

It is ethically and economically questionable:

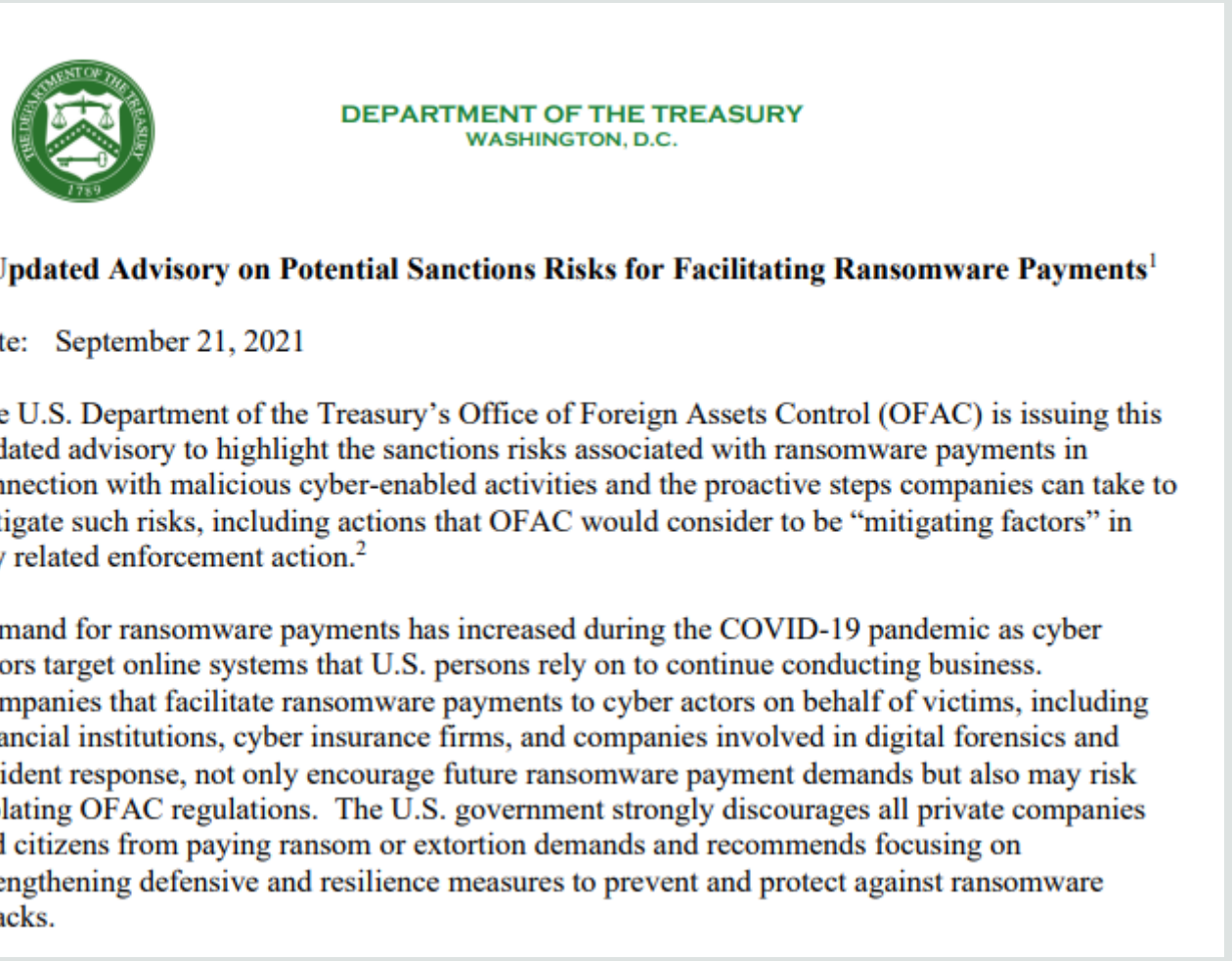
- It funds the attackers
- Links have been identified between cybercriminal activity, organized crime, and terrorist organizations:
  - Funds criminal activities including human trafficking, drug trafficking, weapons trafficking, counterfeit goods, and terrorism
- Authorities in Canada and the U.S. typically recommend not to pay the ransom

Why not just pay the ransom?

It is encouraging them:

- They come back
- They increase their demands if they know you can afford it

Increasing Legal Risk for Paying Ransoms



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

Source: U.S. Department of Treasury

State of Ransomware Survey

- Of the 5,600 organizations surveyed, almost 4,000 (66%) suffered a ransomware attack
- Of those, 1,700 (46%) paid the ransom but either some or all of the data was corrupted or double-encrypted
- On average, 61% of encrypted data was restored after paying the ransom (down from 65%)
- Just 4% got all their data back undamaged (down from 8%)

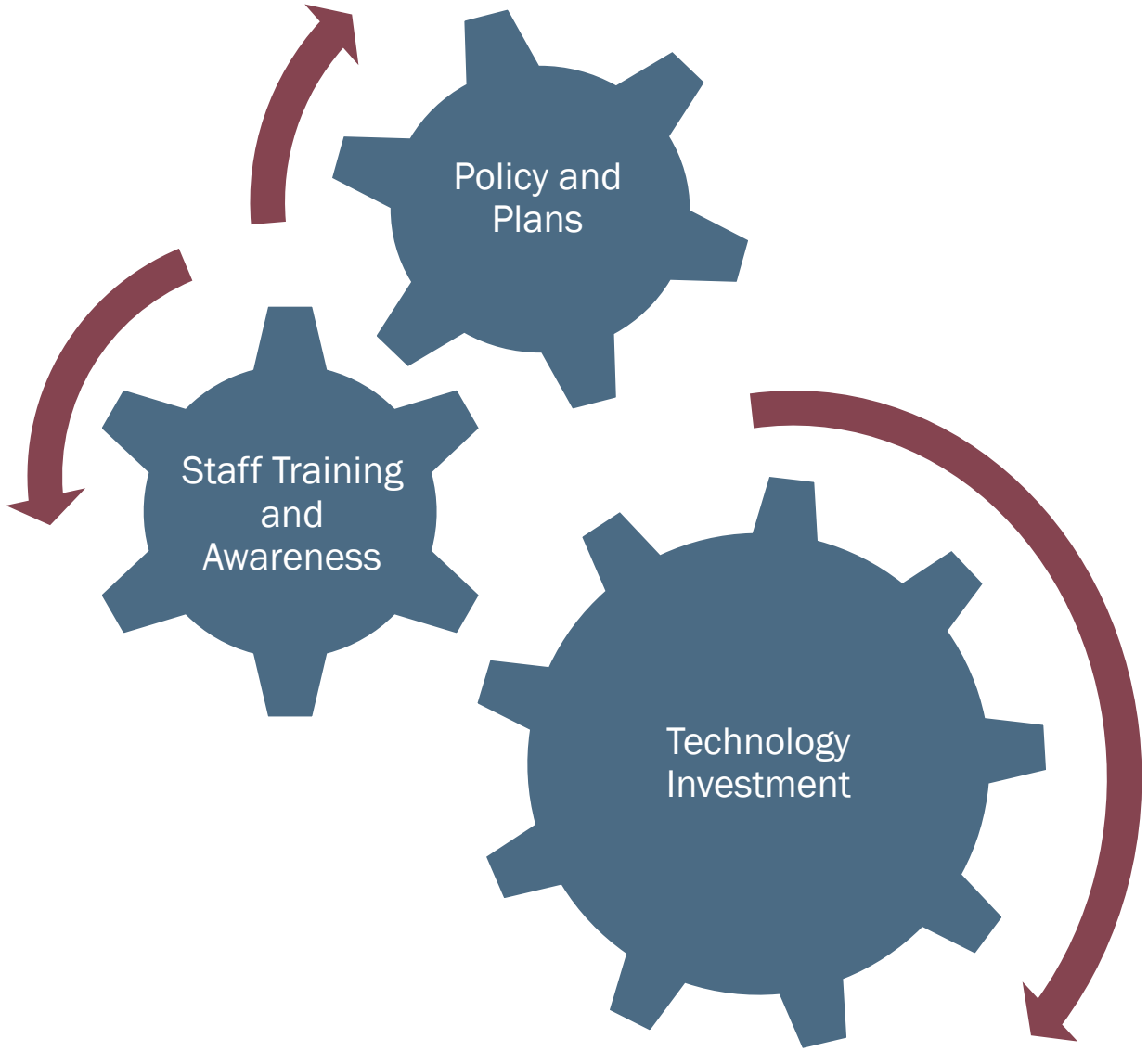
Source: Sophos — The State of Ransomware 2022

Recap

- ❑ Attacks are becoming increasingly complex, effective and costly
- ❑ Criminal factions behind them are more organized, more “professional”
- ❑ Smaller enterprises are on average the most severely impacted, having fewer defenses and less resilience to catastrophic events
- ❑ Brand and financial damage from an attack can be considerable

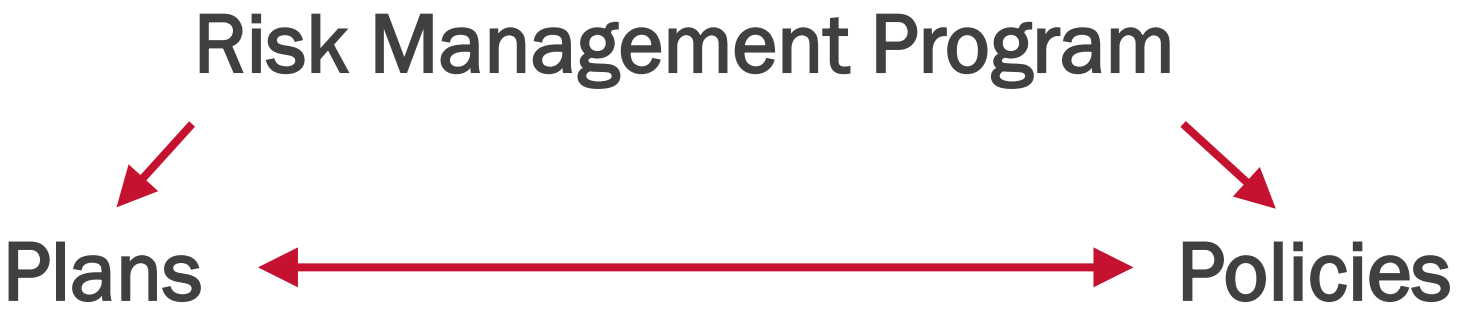
What to do

The Three Pillars of Risk Governance



Checklists

Policies and Plans – Top Picks



1. Incident Response Plan (IRP)
2. Business Continuity Plan (BCP)
3. Information Security Plan
4. Asset Management Plan
5. Vendor Risk Assessment

1. Privacy Policy
2. Computer, Mobile, and USB Device Policy
3. Password Policy
4. Data Encryption and Backup
5. Email Use / Social Engineering Awareness

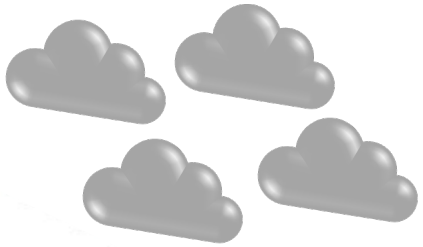
Train Your Staff

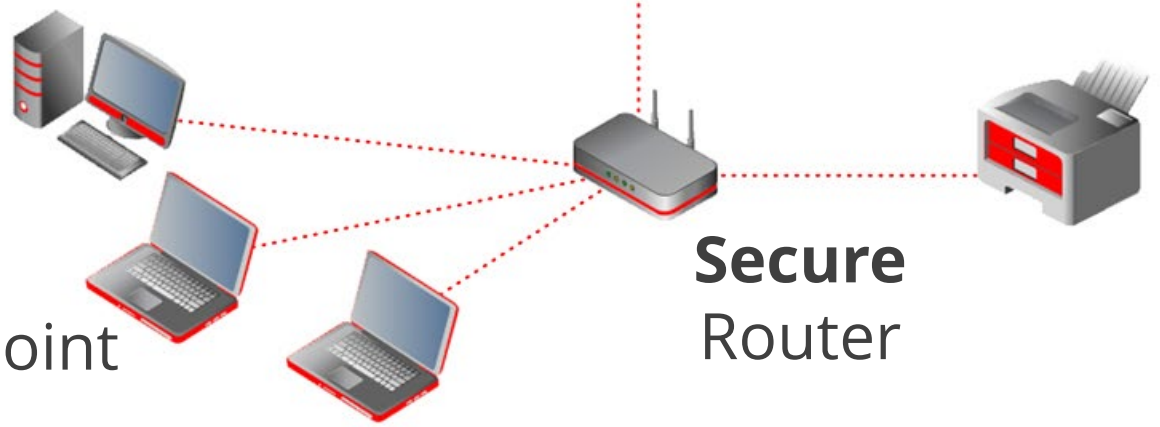
- ❑ Have clear policies in place for computer use, passwords, information handling, etc.
  - ❑ Don’t click what you don’t know:
    - ❑ Links or attachments in unexpected emails
    - ❑ Websites you are uncertain of
  - ❑ Observe error and warning messages from your computer
  - ❑ Observe email addresses
  - ❑ Establish email source and address verification process
- ❑ Conduct phishing and policy challenges

Save this **checklist** for later.

Office of the Future

Secure Cloud
File storage/
application hosting



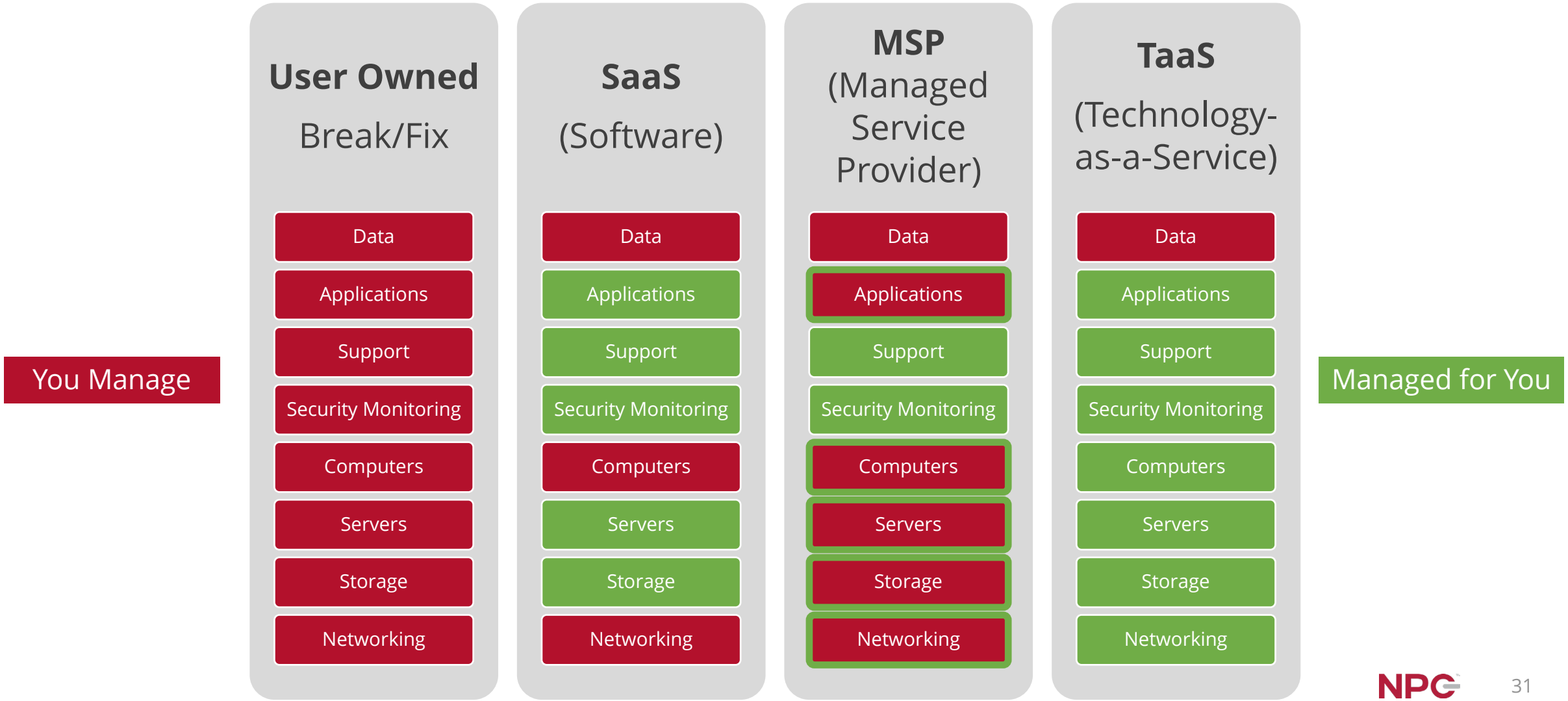


Secure Printer,
Copier, Scanner

Secure
Router

Secure Endpoint
Devices

IT Delivery Models



Protect Your Company

- ❑ Enable Multi-Factor or Two-Factor Authentication
- ❑ Conduct a risk assessment, preferably using a security professional
- ❑ Acquire a specific cyber package, in addition to your E&O or general liability package

Save this **checklist** for later.

Additional Resources

NPC Webinars Recordings

npcdataguard.com/webinars

Enhancing Password Security and the Power of MFA

How to Protect Your Business from Email Compromise Attacks

Protecting Your Identity Online

Building an Incident Response Plan for the SMB

+ New topics added regularly!

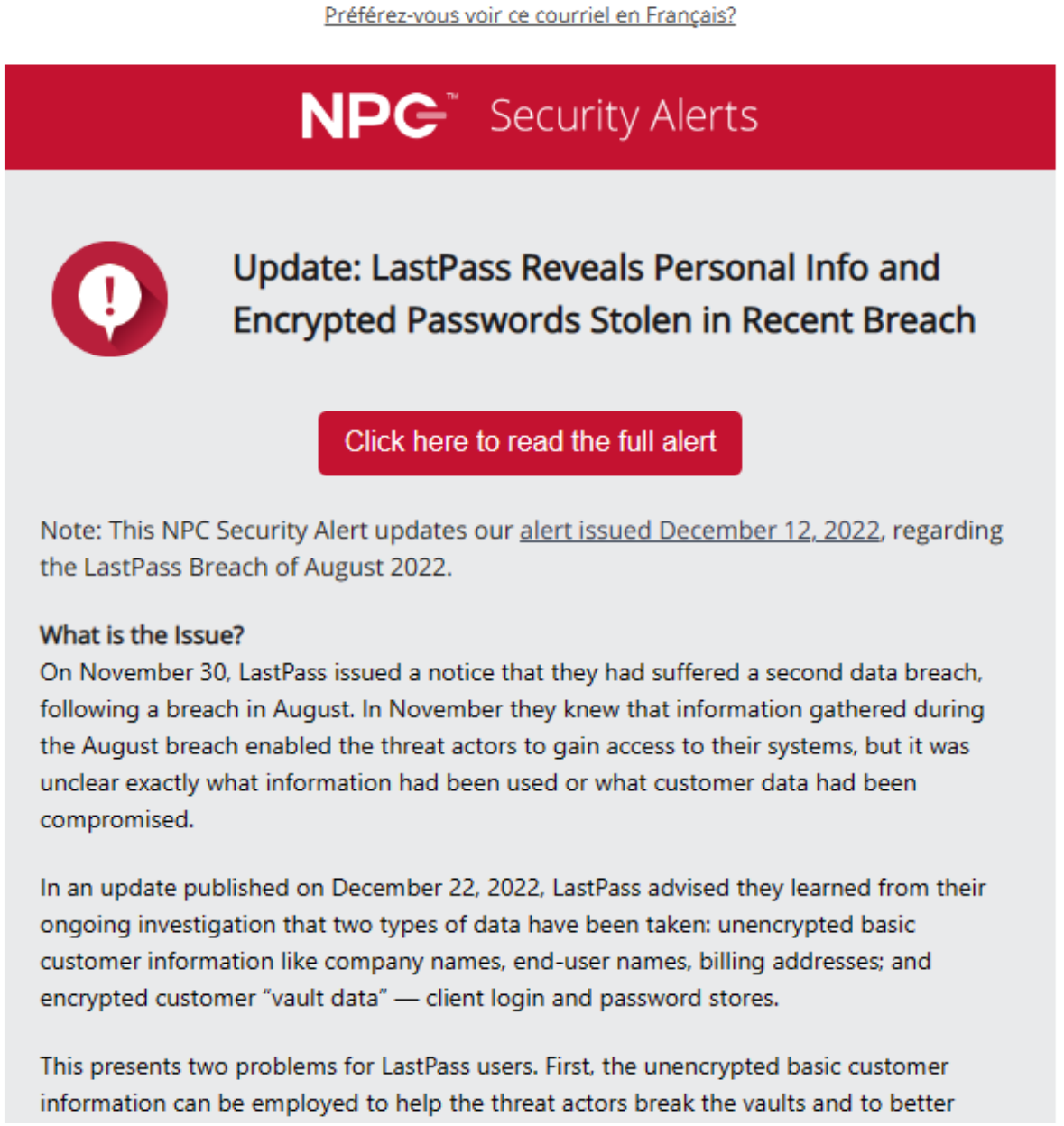
Upcoming NPC Webinars

npcdataguard.com/webinars

February 16th 1:00 PM ET (30 min)	NPC DataGuard Solutions Overview
March 14th 1:00 PM ET (60 min)	Data Breaches1.0: How to Avoid Becoming a Prime Target
March 16th 1:00 PM ET (30min)	NPC DataGuard Solutions Overview

NPC Security Alerts

npcdataguard.com/alerts



Préférez-vous voir ce courriel en Français?

NPC™ Security Alerts

Update: LastPass Reveals Personal Info and Encrypted Passwords Stolen in Recent Breach

Click here to read the full alert

Note: This NPC Security Alert updates our alert issued December 12, 2022, regarding the LastPass Breach of August 2022.

What is the Issue?

On November 30, LastPass issued a notice that they had suffered a second data breach, following a breach in August. In November they knew that information gathered during the August breach enabled the threat actors to gain access to their systems, but it was unclear exactly what information had been used or what customer data had been compromised.

In an update published on December 22, 2022, LastPass advised they learned from their ongoing investigation that two types of data have been taken: unencrypted basic customer information like company names, end-user names, billing addresses; and encrypted customer "vault data" — client login and password stores.

This presents two problems for LastPass users. First, the unencrypted basic customer information can be employed to help the threat actors break the vaults and to better

Q&A

Larry Keating
lkeating@npcdataguard.com
905-305-6501

Darren Mar
dmar@npcdataguard.com
905-305-6513

Thank You

Please Be Safe & Stay Healthy

NPC™
Smarter Computing

Protect Your Endpoint Devices

- ❑ Ensure you have up-to-date and fully patched:
  - ❑ Computer BIOS, operating system, Office suite
  - ❑ System apps like Java and Adobe
  - ❑ Web browser
  - ❑ Anti-malware suite
- ❑ Enable encryption, and manage it carefully
- ❑ Enable personal firewall on endpoint computers
- ❑ Change default passwords on all IoT devices
- ❑ Only do your work on a secured device

Save this **checklist** for later.

Protect Your Systems

- ❑ Apply principles of least privilege for user access, lock admin accounts
- ❑ Create login segmentation between servers and systems
- ❑ Employ adequate spam email filtering and content scanning, provided by your ISP, email service, or optionally on your firewall
- ❑ Ensure all your web connections are https
- ❑ Use a VPN if you are still accessing a private server or using public Wi-Fi
- ❑ Ensure you have a professional look at your remote desktop setup

Save this **checklist** for later.

Backup Your Files

The ultimate failsafe against loss, theft, fire, mechanical failure, human error, viruses, Trojans, malware, etc.

Sometimes necessary for regulatory compliance.

- ❑ Make sure your backup will restore
- ❑ Do not keep your backup in the same place as the computer(s) you are backing up
- ❑ Ensure you have a backup multiple versions deep, and it connects to your computers only when backing up
- ❑ Distinguish between file sharing, primary storage vs. backup

Save this **checklist** for later.

Secure Your Wi-Fi

- ❑ Ensure that your home Wi-Fi:
  - ❑ Has a strong, long password that has been changed from the default
  - ❑ WPA2 level security is enabled
  - ❑ Disable UPnP - Universals Plug and Play
  - ❑ Disable WPS – Wi-Fi Protected Set-Up
  - ❑ Ensure your home router is patched and up-to-date
  - ❑ The router's firewall, if present, is enabled
  - ❑ Has an obscure SSID, or disable SSID broadcast
- ❑ Change default passwords on all IoT devices

Save this **checklist** for later.

Secure Work From Home Checklist

- ❑ Browsing:
  - ❑ Decline data sharing, restrict cookies
    - A more "personalized" browsing experience is a poor trade-off for your identity
  - ❑ Resist saving credit card information and auto-fill information in your browser
  - ❑ Don’t play, casually browse, or shop on your work computer
- ❑ Ensure your smartphone is secured, consider an anti-malware app for it
- ❑ Don’t forget about physical workspace security:
  - ❑ A separate, low-traffic area
  - ❑ Ensure home bandwidth is adequate

Save this **checklist** for later.

Back