Lunch & Learn

How to Protect Your Business from Cyber Threats Like Ransomware

Atekro

Scott Nelson

Founder & CEO of Atekro

Business owner/entrepreneur

30 years as a software engineer/architect

Built enterprise grade solutions that serve millions of customers

Deep desire to help others succeed

Intense curiosity for anything technology

Thank You!

CITY OF
ISSAQUAH
WASHINGTON

THE GREATER
ISSAQUAH
CHAMBER OF COMMERCE

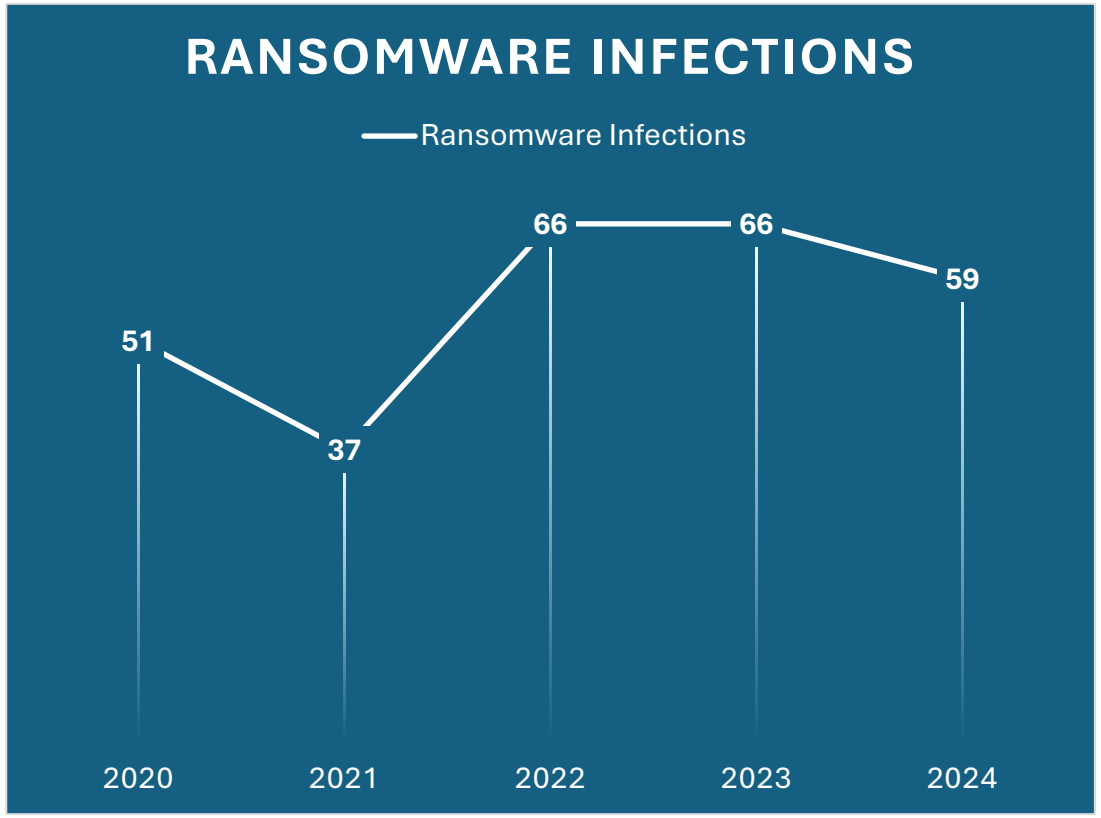
Agenda

- What is Ransomware
- True Cost of Ransomware (Business Impact)
- Ransomware Myths
- Building a Formidable Defense
- Individual Security Protection Components
- Compliance Regulations

What is Ransomware

- A type of malicious software designed to block access to a computer system until a sum of money is paid.

Ransomware Numbers (2024 Report)



% of organizations hit by ransomware

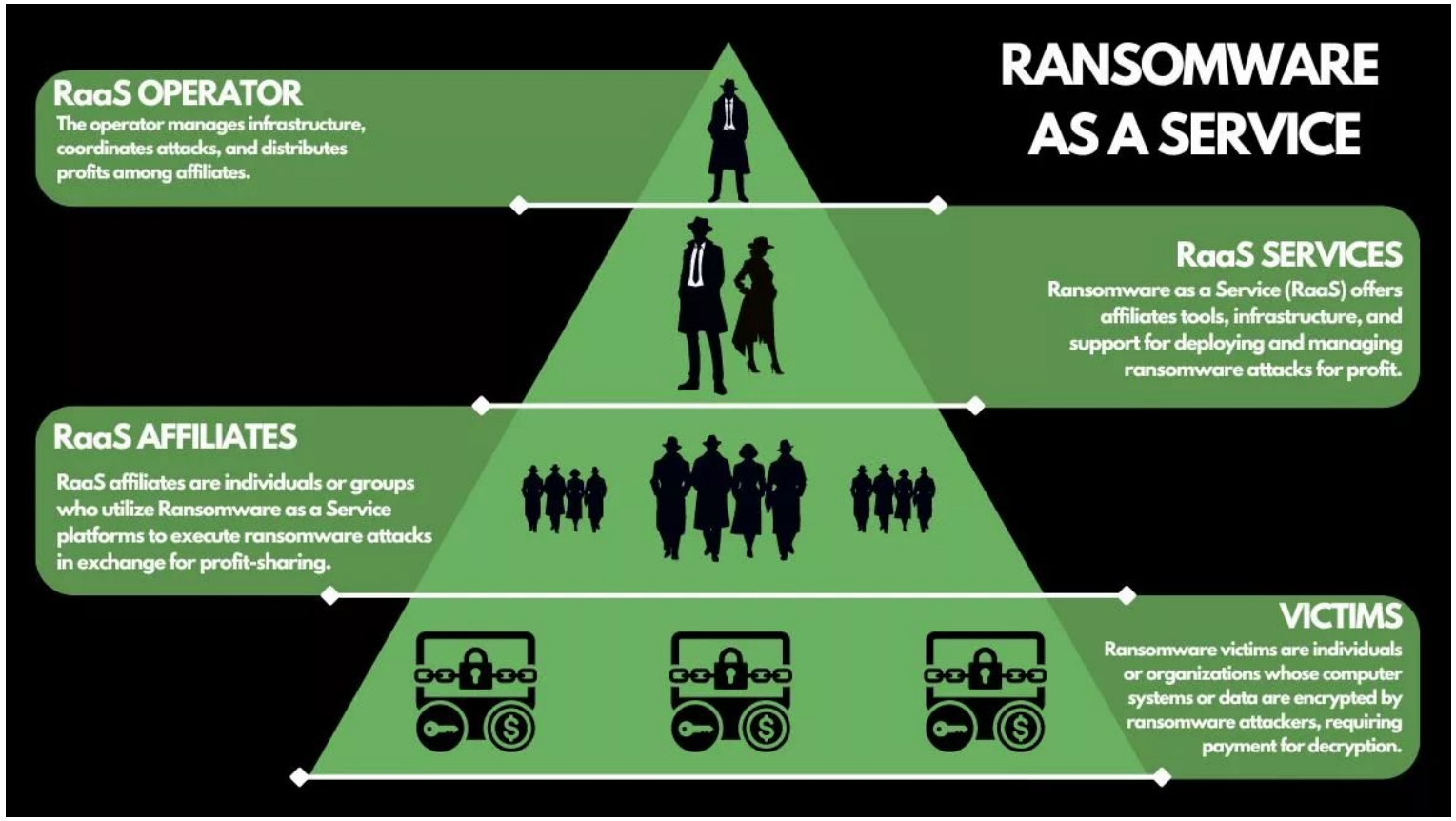
Median	• $ 2,000,000
Mean	• $ 4,321,880

Average ransom demand

2021	2022	2023	2024
$1.85M	$1.4M	$1.82M	$2.73M

Recovery costs (mean)

Ransomware as a Service (RaaS)



Business Impacts

- The ransom
- Cost to recover
- Downtime
- Loss of revenue
- Loss of customer trust
- Legal fees and fine
- Sleepless nights & anxiety

Ransomware Myth or Fact?

We are too small to be a target

FALSE

Ransomware Myth or Fact?

I’ll never get a virus or ransomware with the right anti-virus

FALSE

Ransomware Myth or Fact?

Ransomware only comes from suspicious emails

FALSE

Ransomware Myth or Fact?

Paying the Ransom will solve the problem

FALSE

Ransomware Myth or Fact?

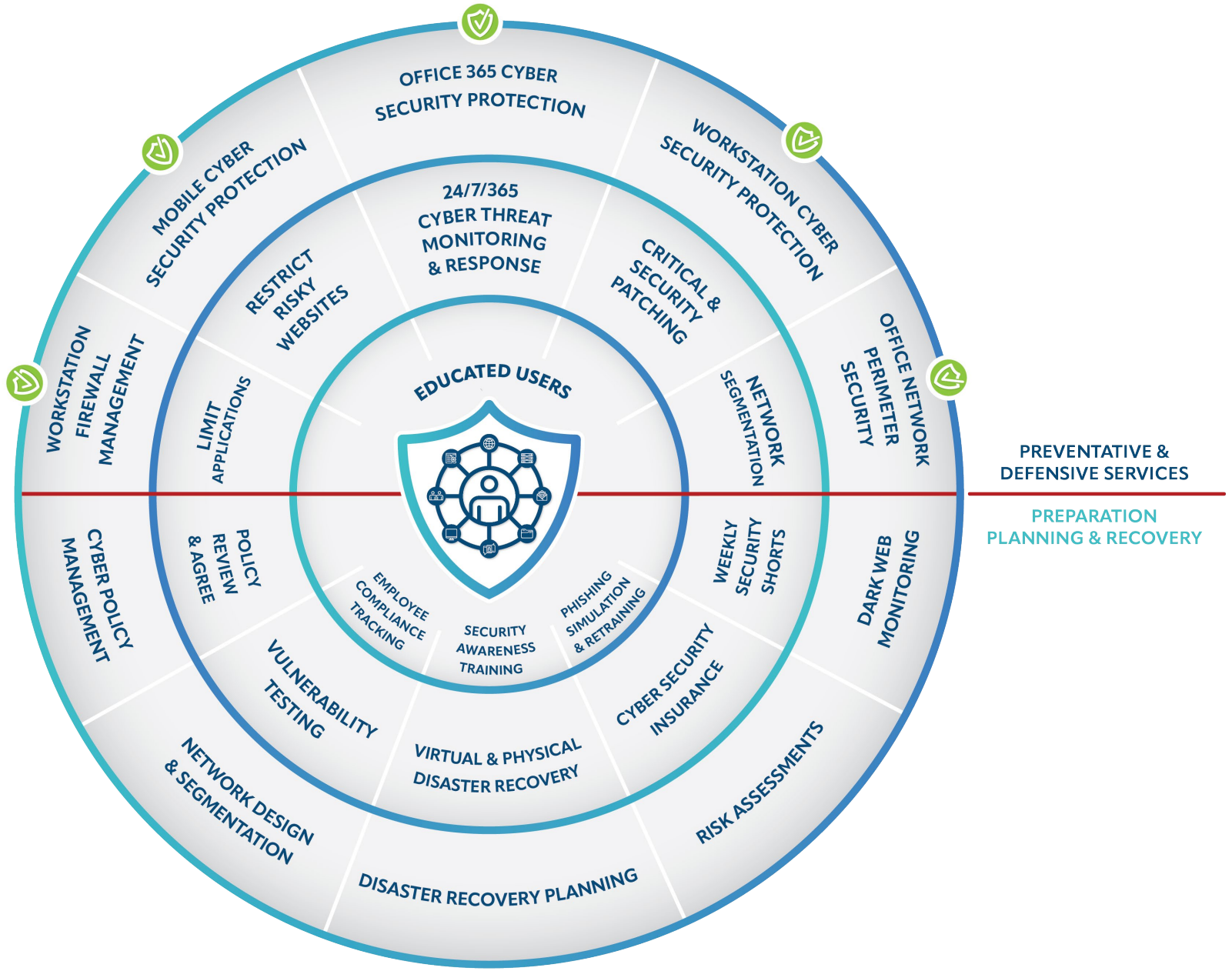
Backups make us ransomware-proof

FALSE


Protecting
Your Business
from
Cyber Threats!

Cyber Security Protection Strategy

- No one layer is 100%
- Multiple layers reduce the chance of infection
- Addresses multiple attach vectors



Building a Formidable Cyber Defense Plan

- Perform a risk assessment
- Address all attack vectors
- Turn on MFA for everything
- Monitor and take quick action
- Exercise least privileged principles
- Segment your network
- Have a backup & recovery plan
- Educate your employees
- Purchase cyber security insurance

Implement Email Security

- Detect phishing emails
- Scan for infected attachments
- VIP impersonations
- Compromised links
- Implement SPF, DKIM, & DMARC protocols

Protect all Computer and Mobile Devices

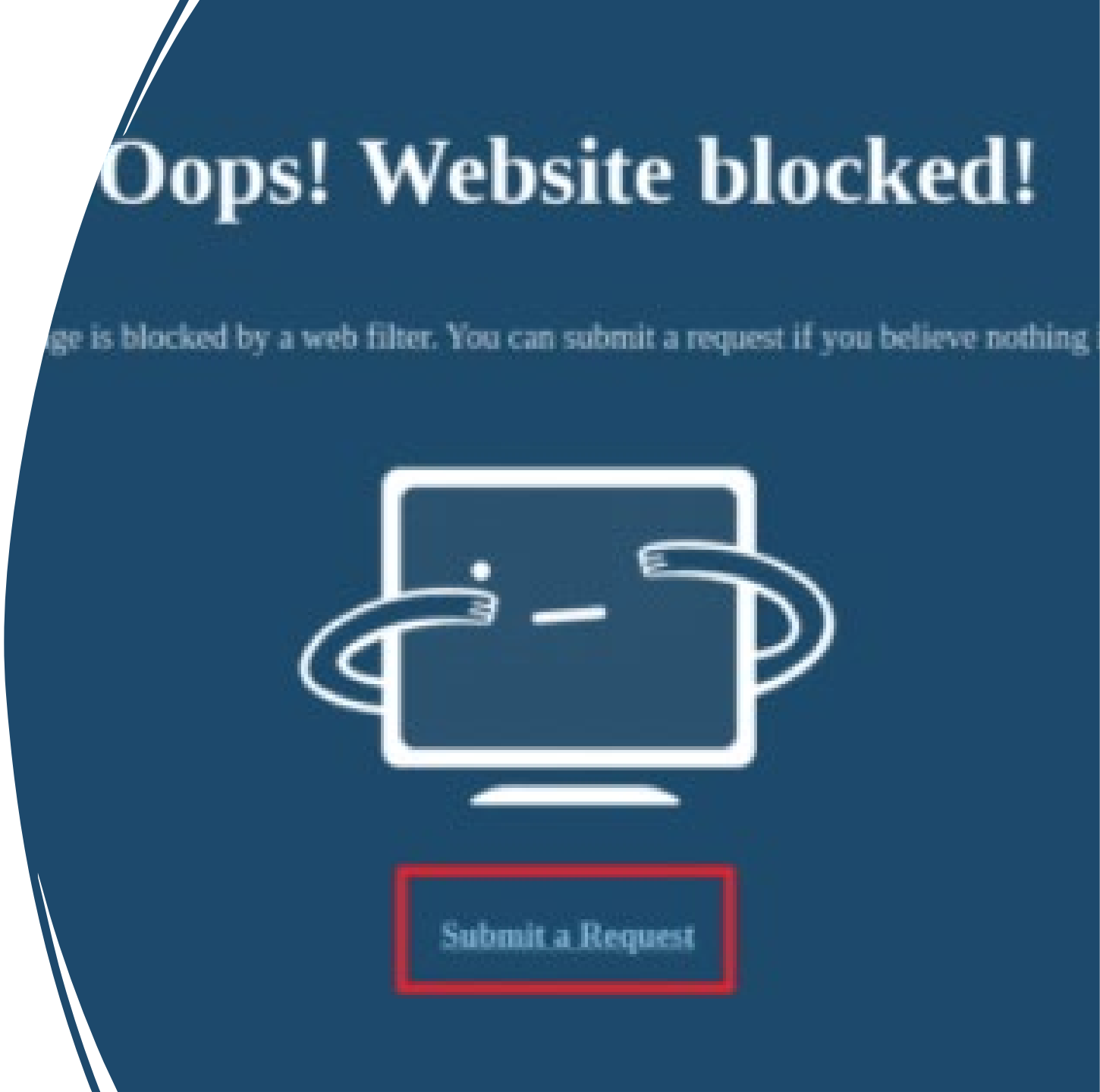
- Deploy advanced an EDR/XDR Anti-Virus
- Not only scan files, but detect behavior using advanced AI/ML technology

SOC Center Monitoring 24/7/365

- Security Operation Center
- Cyber security human experts
- Most threat actors will attack during off hours and holidays
- Quick action is key

Web Content Filtering

- Restrict risky & unwanted websites
- Follow me filtering



Patch Software & Hardware Frequently

- Close vulnerabilities before malware can exploit it
- Ensure all devices are regularly patched
- Patch all critical & security vulnerability quickly

Backup & Recovery

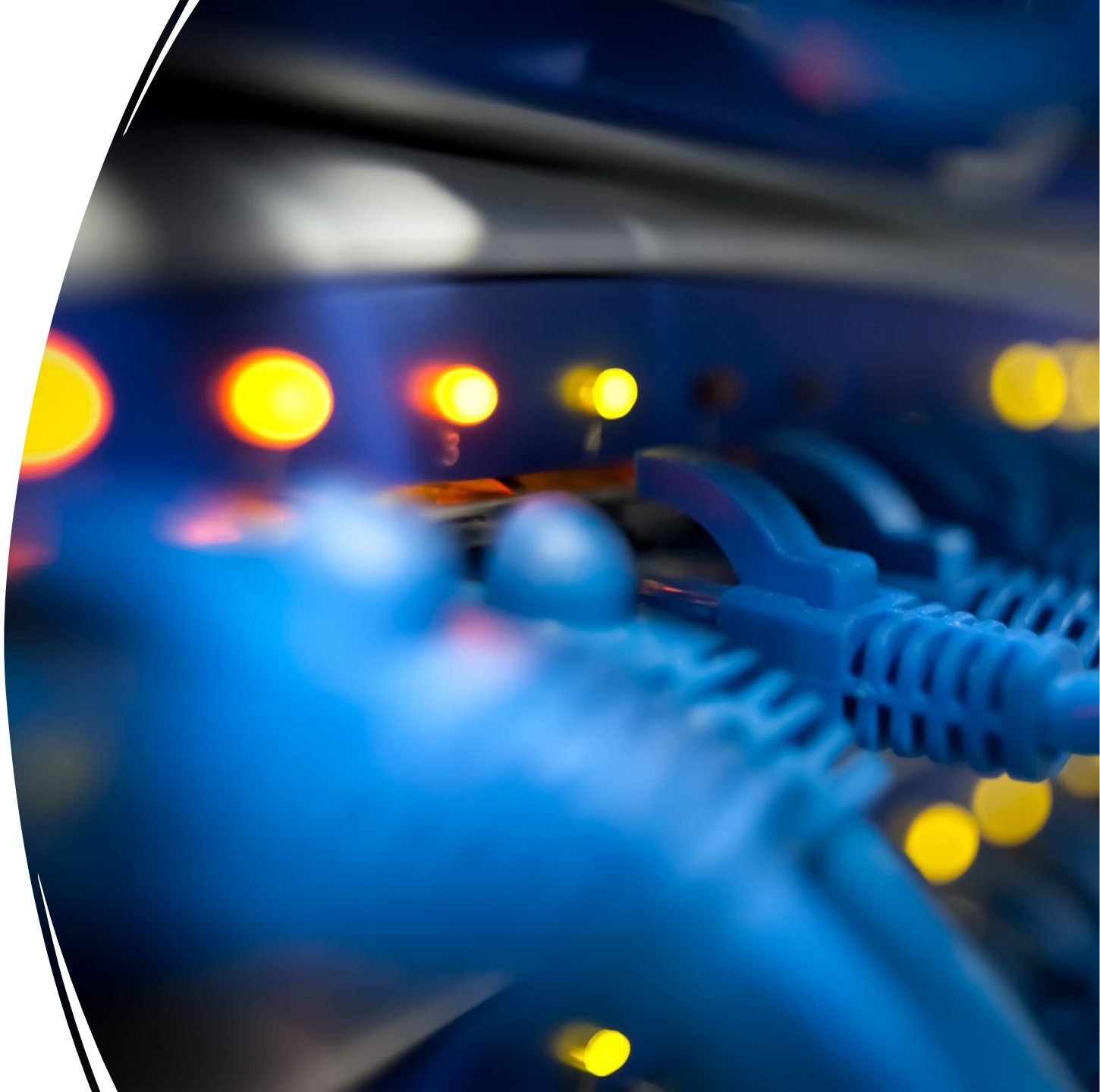
- Have a plan!
- Utilize fast virtual recovery cloud services
- Good for any disaster, not just ransomware
- Have multiple copies of backups (local, cloud)
- Ensure all backups are immutable

Least Privileged Principle (Zero Trust)

- Only allow enough access for employees to do their job
- Only allow required applications & block all others
- User should never have administrative rights on their workstations

Protect your network

- Segment your network
- Use Next-Gen Firewalls
- Do not allow unauthorized devices (zero trust)
- Use secure VPNs for access



Educate Your Employees

- Yearly security awareness training
- Review & acknowledge cyber policies
- Simulated phishing emails
- Regular security updates (weekly security shorts)

Purchase Cyber Security Insurance

- Covers recovery costs
- Has their own protection requirements

Others Best Practices

- Culture of cyber threat awareness
- Monitor the dark web for breaches
- Perform PEN and/or vulnerability tests regularly
- Review your security plan at least once a year
- Perform a risk assessment at least once a year or when ever anything changes in your network

Incident Response

What to do if you get hit

- Isolate infected system **immediately!**
- Do **NOT** pay the ransom
- Report to the appropriate person and/or authorities
- Begin restoration plan from backups
  - virtual recovery
  - physical recovery

Compliance Regulations

- Companies are NOT protecting their customers data
- Government regulatory are getting involved
- FTC Safeguarding Rule

Questions?

THANK YOU!

Atekro

For more information, please contact:

Scott Nelson
Scott.Nelson@atekro.com