Cybersecurity in a Post-pandemic World

BerryDunn

Christopher S. Ellingwood

Ransomware - Modern Day Piracy and What You Can Do

Christopher S. Ellingwood

Learning objectives

- **Understand** the risk of ransomware and how it has heavily impacted healthcare and not-for-profit organizations
- **Learn** things you can do to help prevent attacks from happening to you

Agenda

1. What exactly is ransomware?
2. Case study – UVM Health Network
3. Case Study – Not-for-profit attack
4. Techniques to Mitigate Risk

Polling question #1

What is ransomware?

- Hackers take control of your systems and hold them hostage until you pay them to turn it over to you. In some cases hackers start deleting data and raising price to motivate you to pay up.
- Two ways to get infected – a user downloads software and/or hackers take control of your systems remotely and lock you out.
- Complicated and uncrackable encryption.
- Generally speaking, software is installed somewhere – by an unsuspecting user or a hacker.
- In 2020, ransomware cost US organizations $20 billion (that's nearly double 2019).

Where does ransomware come from?

- Ransomware is a software, or macro, that is installed on a user's PC (Forbes poll in 2021: 1 in 5 Americans are victims of ransomware).
- Usually initiated through a phishing scam/attack.
- Cerber “ransomware as a service” – third-party hacker group who has made millions selling a virus that focuses on Office365 vulnerabilities.
- Criminal organizations – modern day pirates; data is worth more than ships.
- Spam e-mail – tricks users to enable macros (automated backend computer process).

How does ransomware spread?

Networked computers – once on network, spreads by taking advantage of known vulnerabilities.

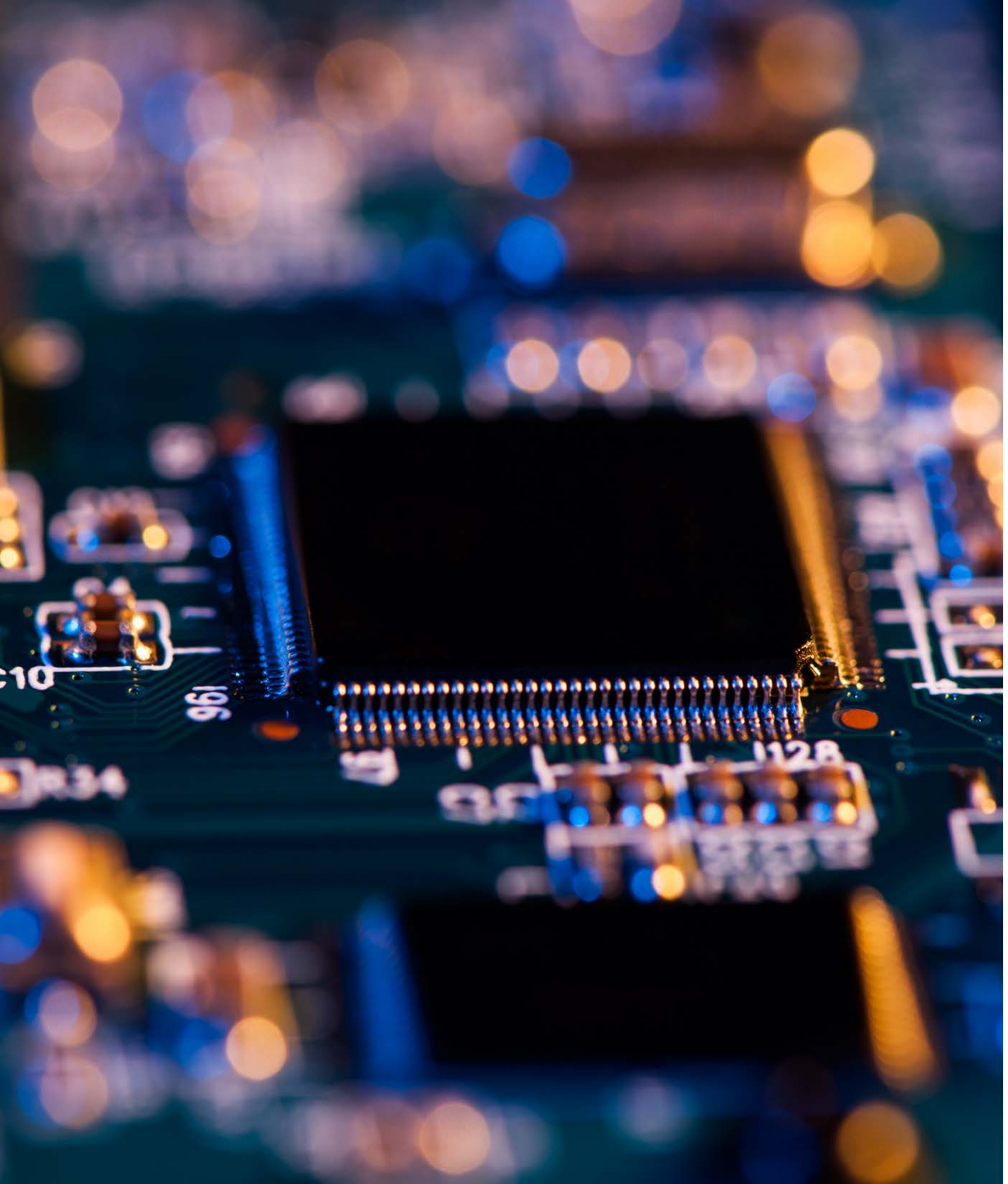
Within software, hackers install key loggers and obtain passwords to user accounts and manually take over systems.

Within phishing emails, tricks users to perform tasks that allow malware to spread.

Case Study: University of Vermont Health Network

The Attack

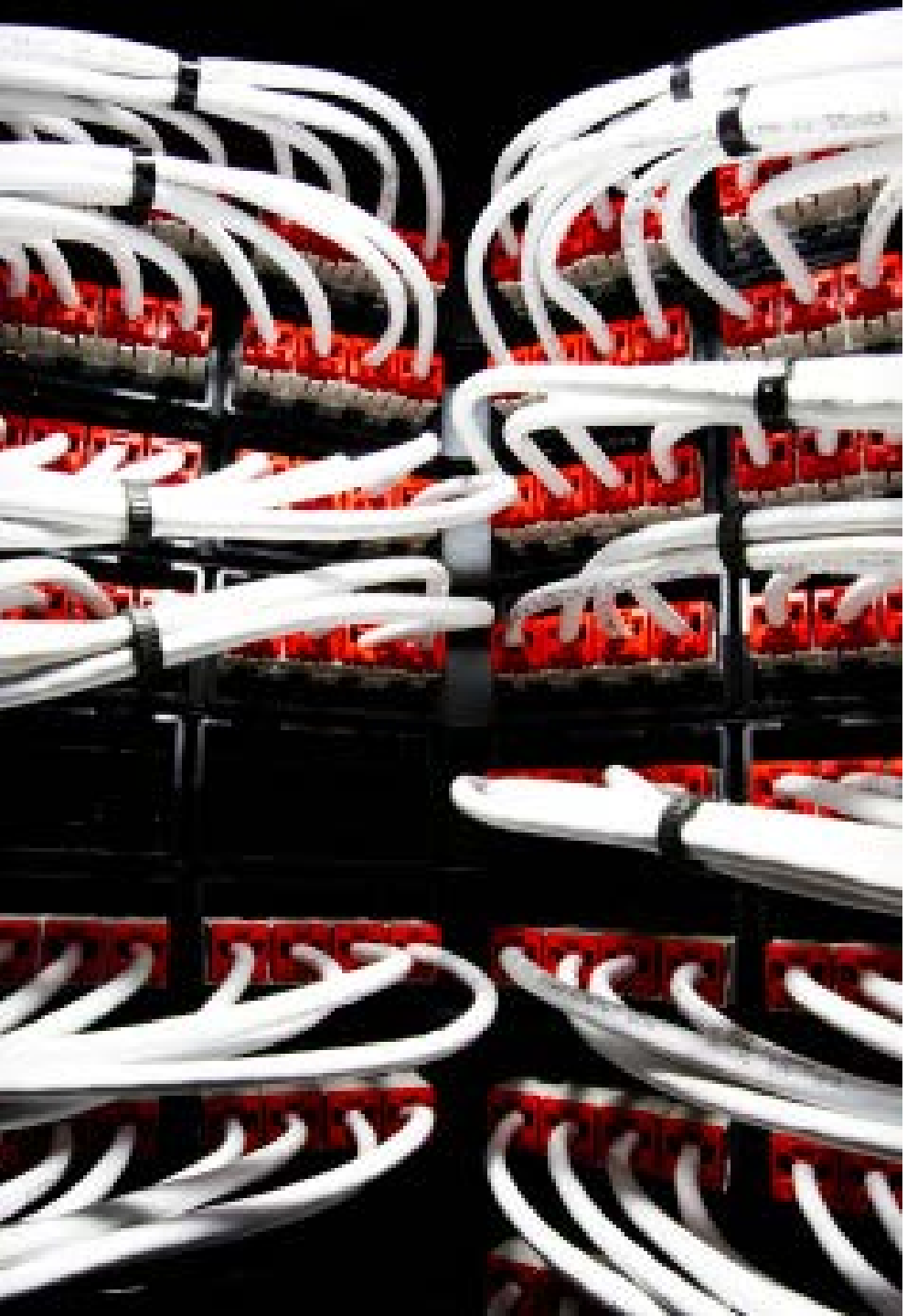
1. October 2020 – Hackers infect UVHN with ransomware software and shut down healthcare applications (core health record system).
2. Hackers successfully infect all 5,000 networked devices in healthcare system.
3. Entire health network is without electronic system access. Providers move to paper charts.
4. In particular, the Cancer Center was severely impacted.
5. This was a known successful version of ransomware called “Ryuk” and has been attributed to Russian hackers who have collected over $61 million in ransom in 21 months.
6. 300 IT professionals and 10 members of National Guard responded and were forced to rebuild 1,300 servers and 5,000 workstations.
7. Unique to this case was there was no overt demand for ransom.



Case Study: University of Vermont Health Network

The Impact

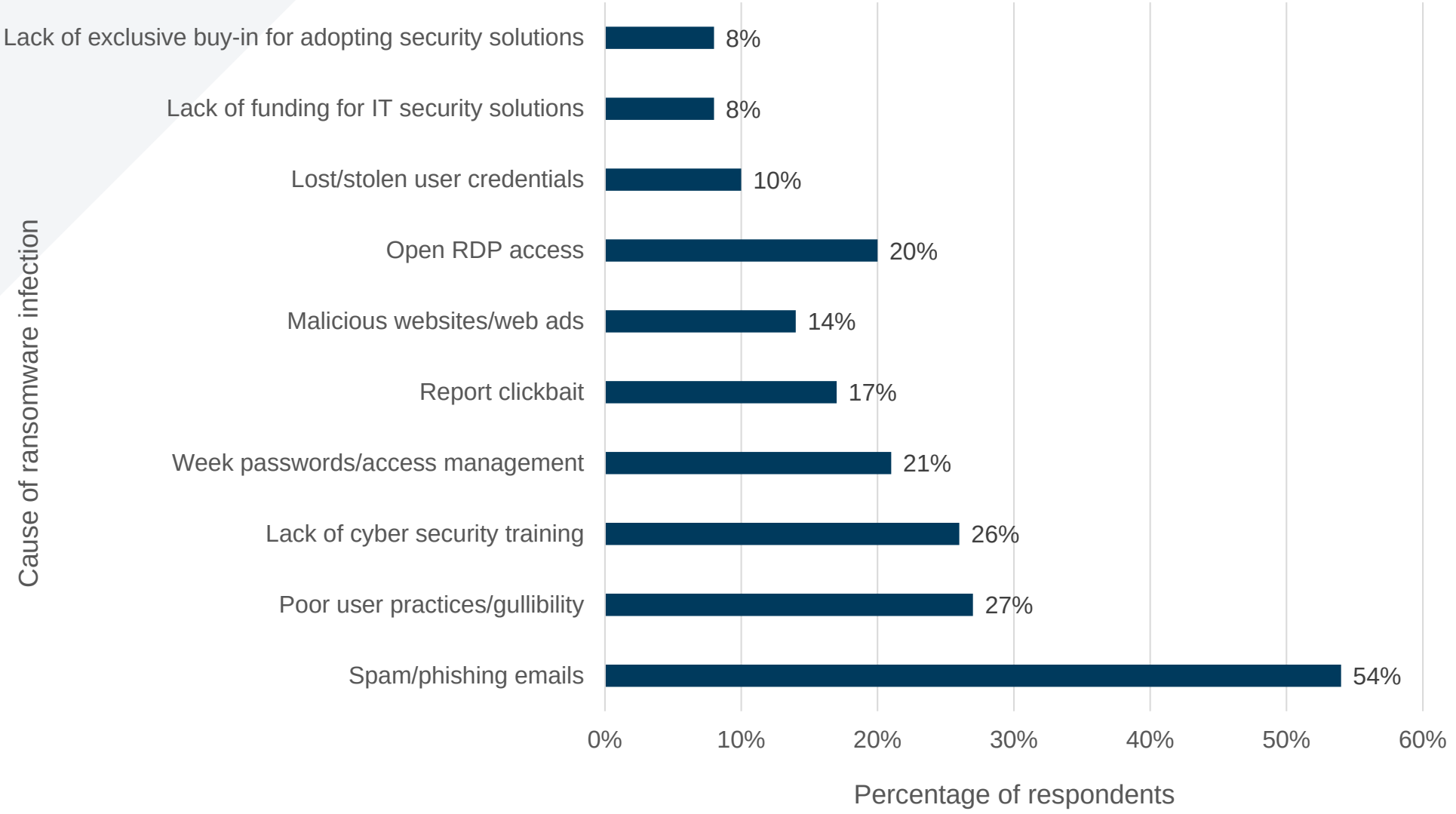
- Systems were down for three weeks. By January 2021 were only at 70-80% restored.
- 300 employees were furloughed because of stopped services due to hardware and systems being unavailable.
- Lost an estimated $1.5 million a day in revenue.
- Current remediation costs (not including lost revenue) is estimated at $64 million.
- UVHN had good controls in place.
- It does not appear that patient information was breached or stolen.
- Key for successful recovery was excellent backup controls.



Case Study: Blackbaud Ransomware and Breach

- February 2020 Hackers access Blackbaud servers and begin stealing data.
- Was not discovered by Blackbaud until May 14, 2020.
- It is estimated that data of over 25,000 Blackbaud customers' (donor information) was stolen by the hackers. This includes 10 healthcare systems and many universities.
- Blackbaud paid the ransom to get the data back. The amount is unknown as Blackbaud has been incredibly secretive over what happened.
- Blackbaud claims it confirmed once ransom paid, stolen data was destroyed – which is malarkey.
- Multiple class action lawsuits have been filed.
- NFPs throughout US have been impacted from lawsuits, having to pay for identify protection, and being overwhelmed by calls from concerned donors.

How does Ransomware get into systems?



Polling question #2

How We Can Mitigate

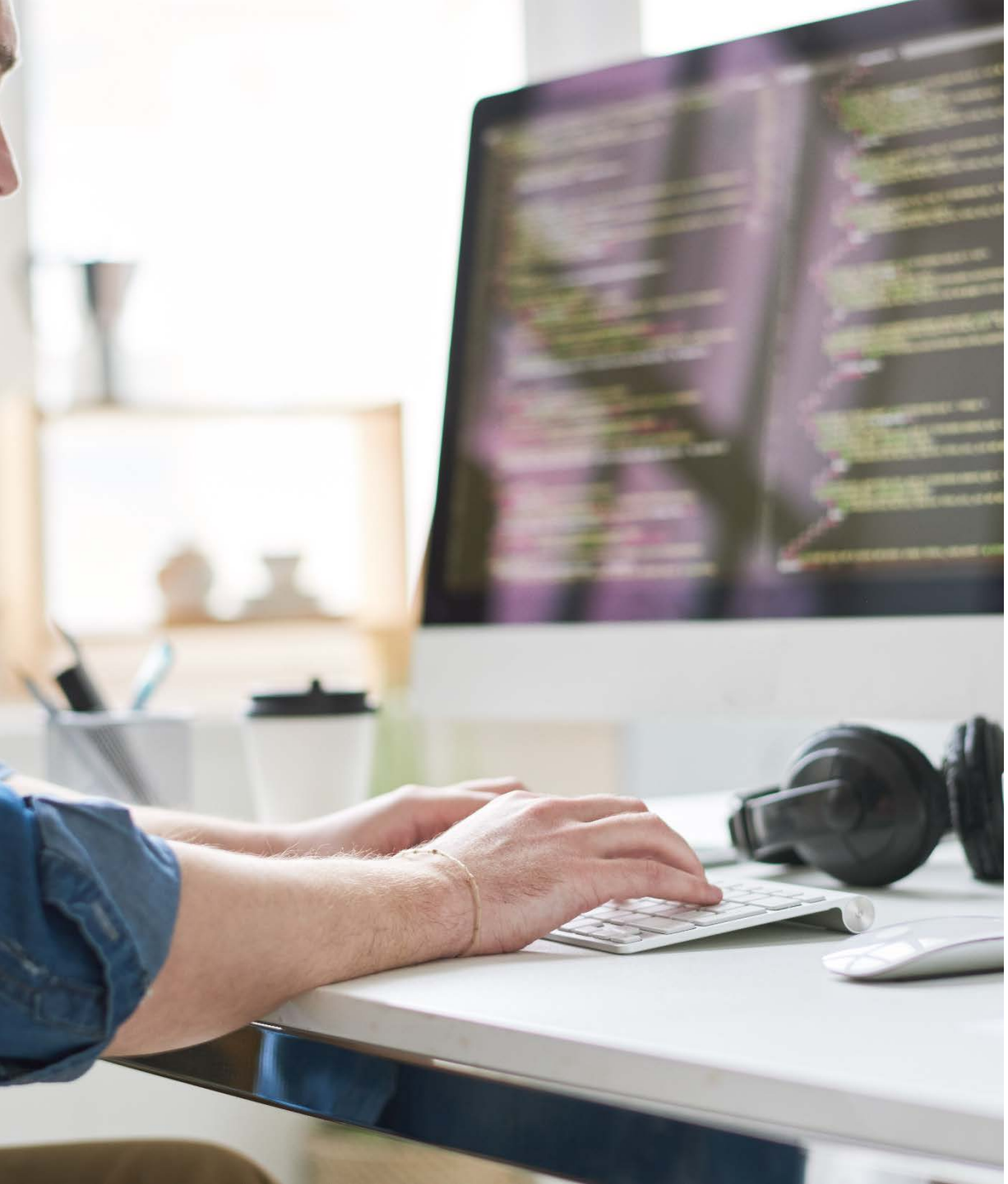
Train and Test

Employee IT training

Focused on phishing and e-mail awareness.

TEST your employees

Yes, you will hurt feelings and people will feel targeted.



How We Can Mitigate

Control Devices

- Remove administrator rights from local machines for users. This prevents them from installing software.
- Disallow macros to be enabled from emails.
- Make sure employees are not using personal workstations (some exceptions may occur).
- Whitelisting software.
- Advanced anti-malware software that is centrally managed.
- Consider using a thin-client environment.

How We Can Mitigate

Back Up Files

- Comprehensive backups separated from network. This won't stop the attack, but it makes recovery 1,000,000% easier.
- Test backups for ability to restore data on a frequent basis.
- Train IT staff on restoration procedures – there are ways to take back control (but files may be lost).
- Make sure Incident Response Plans and Disaster Recovery Plans are up-to-date and in place.

How We Can Mitigate

Protect!

- Patch your systems!
- Force patches to go to workstations (managed workstations)
- Monitor patching process to make sure users are protected
- Zero-day patches go in immediately

Questions?

Ransomware is not a joke, but it can be controlled with basic controls.

Christopher S. Ellingwood
207.541.2290 | cellingwood@berrydunn.com

berrydunn.com