Eliza Jennings
choices for aging well

Cyber Threats and Compliance Challenges: How to Manage Technology Risk

Presented by

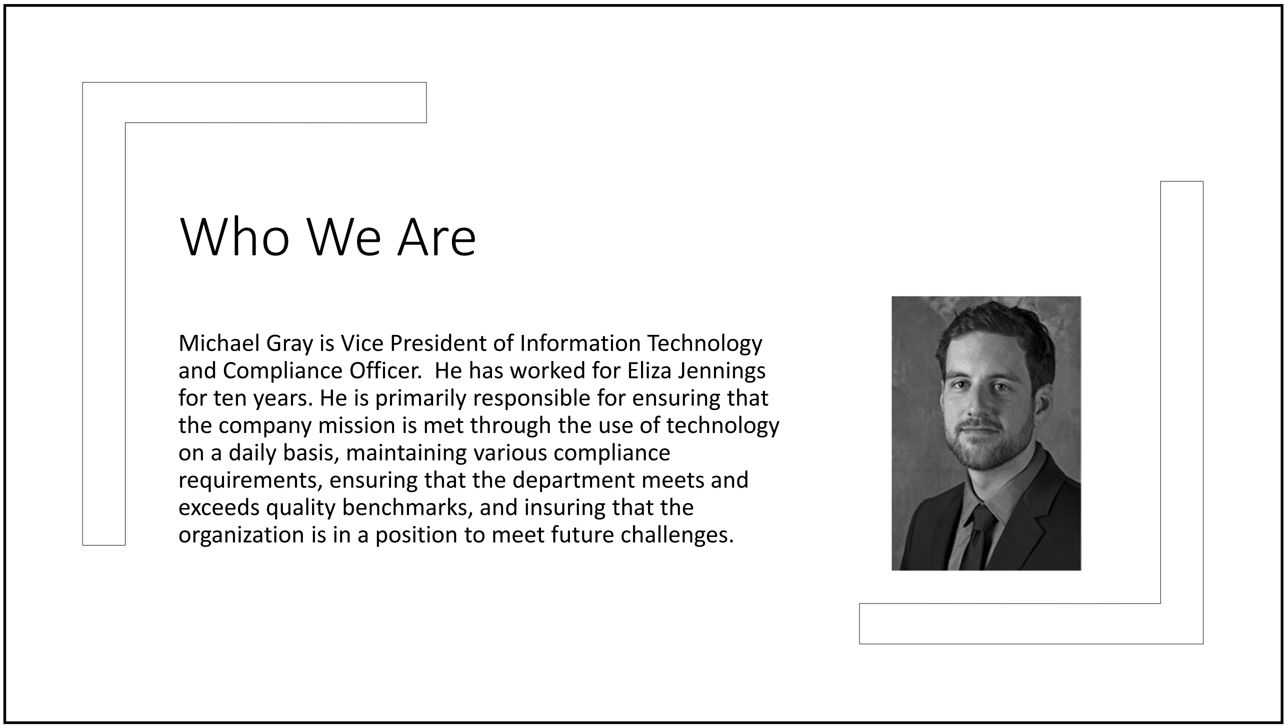
Jennifer Griveas and Michael Gray

1

Who We Are

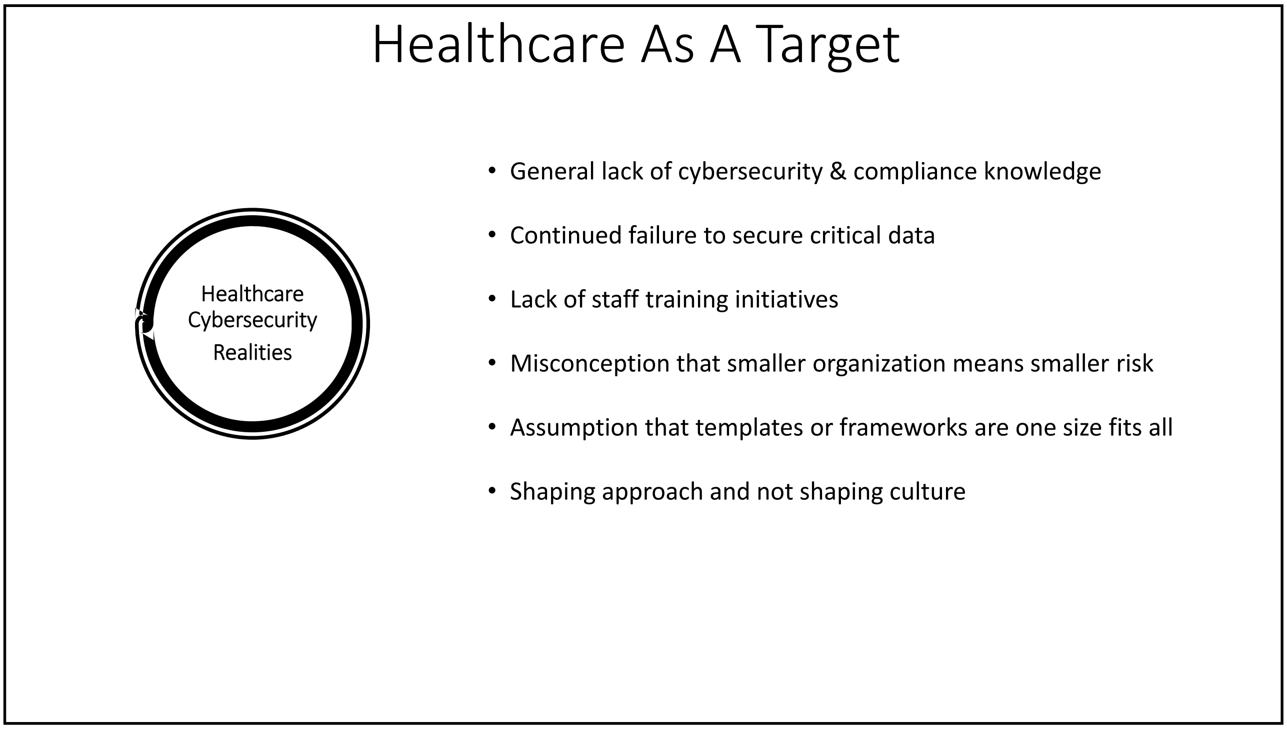
Jennifer Griveas, Esq., CHC, is the Chief Human Resources Officer and General Counsel for the Eliza Jennings Senior Care Network, where she has served as a member of the senior management team since 2011. She oversees all legal matters for the organization, including regulatory compliance and risk management, labor and employment issues, litigation management, and transactional matters. She is certified in health care compliance by the HCCA, and works extensively with company management on matters of compliance and IT security.

2



Who We Are

Michael Gray is Vice President of Information Technology and Compliance Officer. He has worked for Eliza Jennings for ten years. He is primarily responsible for ensuring that the company mission is met through the use of technology on a daily basis, maintaining various compliance requirements, ensuring that the department meets and exceeds quality benchmarks, and insuring that the organization is in a position to meet future challenges.



Healthcare As A Target

Healthcare
Cybersecurity
Realities

- General lack of cybersecurity & compliance knowledge
- Continued failure to secure critical data
- Lack of staff training initiatives
- Misconception that smaller organization means smaller risk
- Assumption that templates or frameworks are one size fits all
- Shaping approach and not shaping culture

Healthcare As A Target

Healthcare Cybersecurity Realities

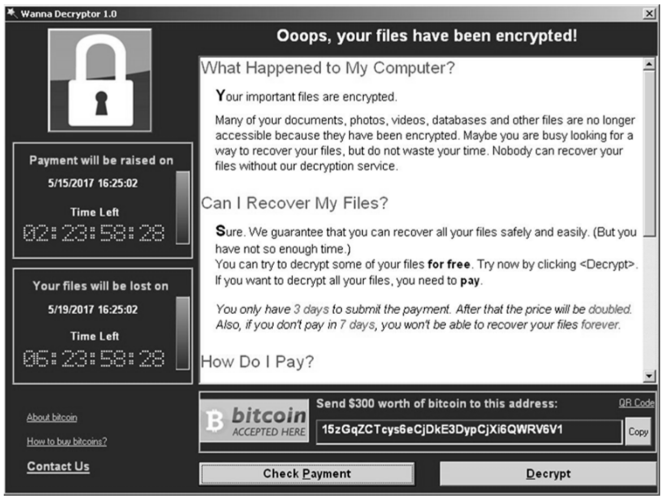
- The healthcare industry ranks fifteenth in terms of cybersecurity health when compared to seventeen other major U. S. industries
- The healthcare industry is one of the lowest performing industries in terms of endpoint security
- Social engineering attacks continue to be a common attack vector
- The most common cybersecurity issues in the healthcare industry relate to poor patching cadence
- Healthcare organizations, even top performers, struggled with patching cadence and network security

5

Top Threats

- Hacking
- Ransomware
- Email
  - Phishing
  - Scams
  - Credential Theft
- External Devices
- Viruses, Malware, and Adware are still concerns, but Ransomware has dominated and is now the most significant threat

6



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Ransomware

New attack every 14 seconds

50% of infections were healthcare

300% more attacks on healthcare expected in 2020

7

The Problem with People

- Insider threats are your biggest risk
- Device loss and theft
- Lack of knowledge and training
- Don’t follow or understand safeguards
- Lack of IT support or IT not at the table
- Don’t know what to do when things go wrong

8

Laws and Other Standards

- Cybersecurity is relevant to numerous regulations
  - Health Care Compliance Plan
  - HIPAA (Privacy and Security Rule!)
  - Requirements of Participation
  - CMS Emergency Preparedness
  - State cybersecurity/data protection laws and consumer protection statutes
  - and more!!

9

Ten things to do right now!

Cybersecurity is an ongoing, constantly evolving effort

Keep informed on emerging threats

You can’t create a cyber compliance program out of thin air. Look to the biggest risk areas as a starting point

10

1. Train. Train Again. Keep Training.

- Staff awareness: know the threats, not just the rules
- Training on hire is only the beginning
- Set work plan for role-based training
- Bite-sized pieces are easier to digest
- Did something go wrong? Time to train. Again. Embrace the repetitive.
- This stuff is fun! It pertains to real life!

2. Policies and Procedures: Make them Meaningful!

- Many statutes **require** written policies
  - Major risk areas require written policies even where policy may not be required by statute.
- Caveat: a policy collecting dust can create bigger problems. Share, educate, update!
- Apply consistently, sanction for violations

3. Get your HIPAA House in Order

- You need a HIPAA Security Rule Risk Analysis and plan to address identified risks.
- The Risk Analysis is the start to a process that never ends
- Risk analysis can be DIY, conducted by a third party, can use or not use HHS tool – but it must be done!
- Identify your Security Officer **and** your key contacts for HIPAA compliance
- Inventory hardware, software, mobile devices
- Security Rule is one part of overall HIPAA compliance – Privacy Rule, Business Associate rules, Breach rules all should factor into that work plan.

4. Manage Mobile Devices

- Get mobile devices under control – know who has them, where they are at all times, and how they can be used
- Develop a mobile device policy. Key considerations:
  - Mobile Device management
  - BYOD
- Encryption – including removable drives!

5. Evaluate your Email

- Who needs it?
- Limit Email rights
- Policy on usage
- Train on common email schemes:
  - Phishing – What it looks like and who to contact
  - Credential Theft – how to spot the trickiest attempts

15

6. Access Controls

- User Accounts require careful creation per policy – avoid the copy & paste approach!
- Account terminations require a STRICT policy that people actually follow!
- PoLP should guide access rights policy
- Auditing – put user account creation and termination review on your work plan
- Admin Rights – Limit, define by policy, and revisit – Prepare to be unpopular!
- Removable drives
- Passwords

16

7. Data Transmission

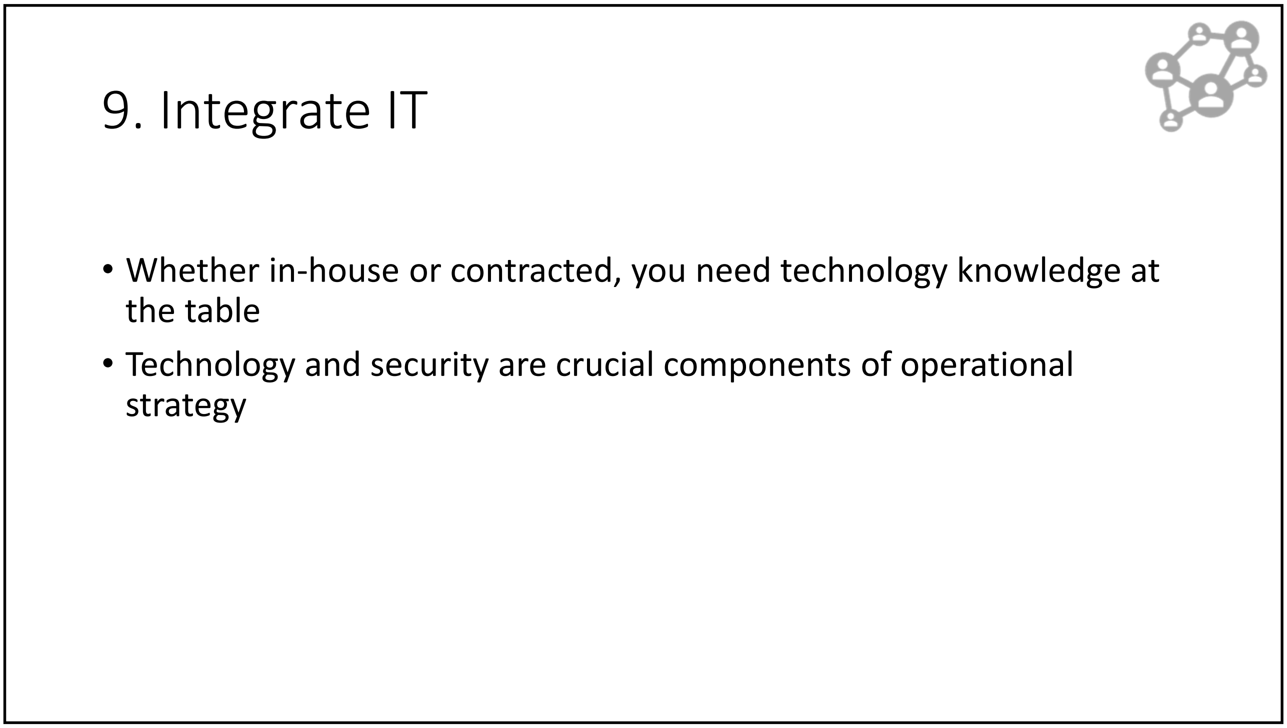
- Data should only be in motion as defined in policy
- VPN for remote use
- Email encryption
- Texting

17

8. Watch out for WiFi

- Open networks can be dangerous
- VPN and data transmission
- Policies and procedures – for use of your WiFi and for your Mobile Devices out in the wild
- Control of WiFi?
  - Separation of networks

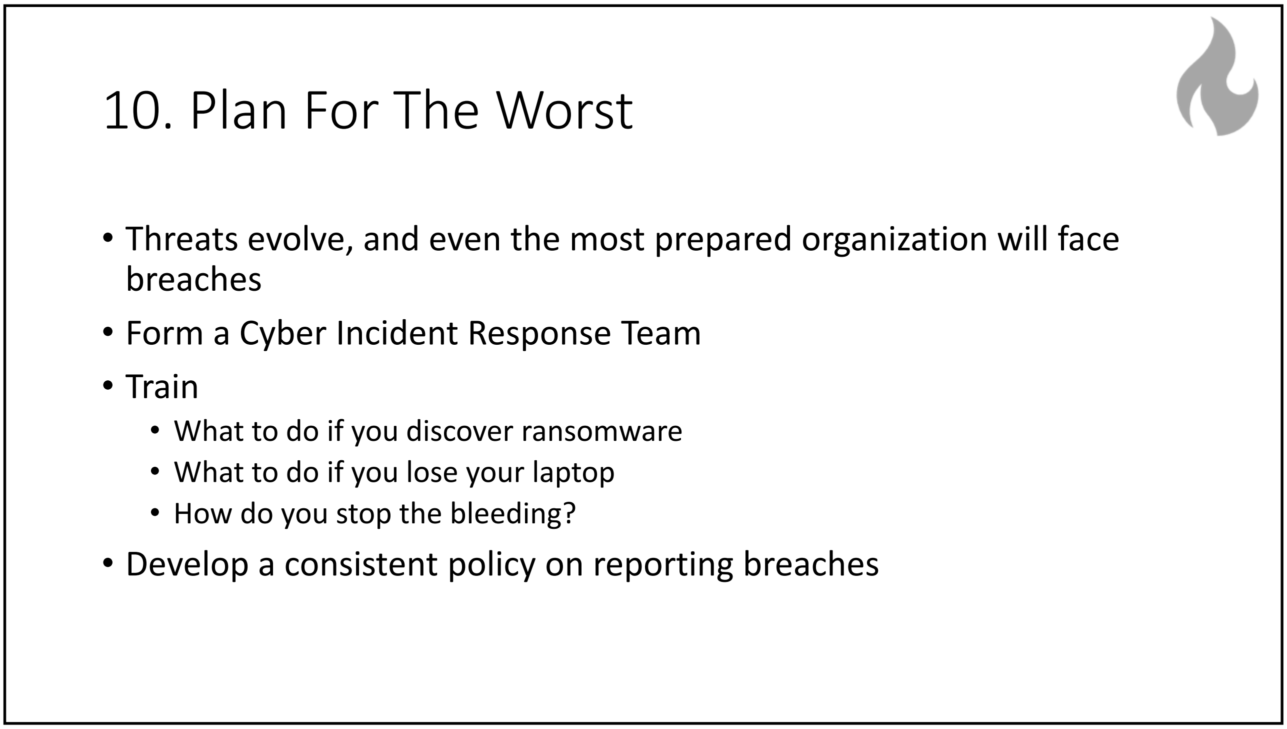
18



9. Integrate IT

- Whether in-house or contracted, you need technology knowledge at the table
- Technology and security are crucial components of operational strategy

19



10. Plan For The Worst

- Threats evolve, and even the most prepared organization will face breaches
- Form a Cyber Incident Response Team
- Train
  - What to do if you discover ransomware
  - What to do if you lose your laptop
  - How do you stop the bleeding?
- Develop a consistent policy on reporting breaches

20

Questions?

21