FORTIFYING CYBERSECURITY IN HEALTHCARE

Don't Just Treat the Symptoms, Address the Cause

AGENDA

MEET YOUR PANELISTS:

ROD VOLZ
Chief Growth Officer at USX Cyber

COLE MCKINIEY
Chief Technology Officer at USX Cyber

FRANK HUGHES
Chief Information Officer at USX Cyber

- What's going on with cybersecurity in Healthcare?
- Compliance by the market, not just the government
- How to find solutions economical for your business
- Recommended approach to compliance and overall protection
- How to plan and prepare for incident response
- Panelist Q&A
- Audience Q&A

1

WHAT'S GOING ON WITH CYBERSECURITY IN HEALTHCARE?
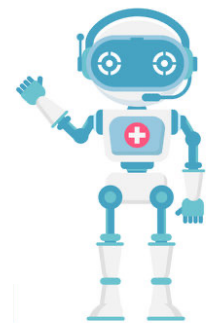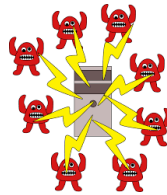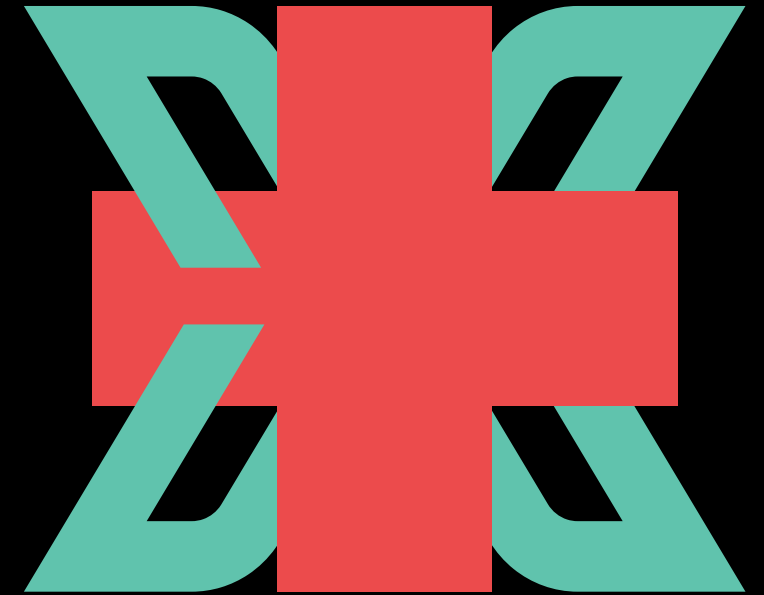
SUPPLY CHAIN
LINKAGES

- Where are YOU in the Healthcare Supply Chain?

- Is your organization being vetted by others consuming your goods and services?

- How are you assessing the cyber 'fitness' of your suppliers and vendors?

Compliance is increasingly becoming the currency businesses rely upon as they manage their supply chain up and down the line.

BUT DON'T JUST COMPLY, BE SECURE!

3

USX
CYBER

AN ESTIMATED

6%

OF HEALTHCARE BUDGET

is allocated towards cybersecurity

Large healthcare organizations understand their need for compliance but it doesn't end with them. Their vendors and suppliers are an integral part to their work as many are beginning to look for compliance up and down the chain now even in the absence of mandatory compliance.

COMPLIANCE FRAMEWORKS

HITRUST

Fast Becoming Compliance Framework
of Choice in Healthcare Industry

2009

Initial version of HITRUST Common Security Framework (CSF) released.

2019

HITRUST CSF gains recognition internationally.

2007

HITRUST Alliance founded with mission of addressing infosec challenges in healthcare industry.

2013

HITRUST collaborates with the U.S. Dept. of Health and Human Services and the Office of Civil Rights to align CSF with HIPAA Security Rule

2023 & BEYOND

The HITRUST Alliance releases v11.2 in October 2023, continuing to enhance and extend the security framework for greater impact and use.

COMPLIANCE DOESN'T MEAN FULL BUSINESS PROTECTION.

While HITRUST controls and artifacts are essential building blocks to cyber maturity, they're not all that you need.

HITRUST compliance is a piece of the puzzle next to cyber hygiene, risk management, cyber insurance and more.

RECOMMENDED APPROACH TO
COMPLIANCE AND OVERALL PROTECTION

Best value obtained when your service provider can work with you end-to-end on your compliance and cybersecurity journey.

This allows you to stay compliant and provides you with the peace of mind that comes with knowing your business is protected from constantly evolving threats.

FULL HITRUST COMPLIANCE

Assessment & Customization

Cybersecurity implementation

Documentation & Procedure

Ongoing monitoring & Response

FLEXIBLE AND CUSTOMIZED SERVICES

HOW TO FIND SOLUTIONS ECONOMICAL FOR YOUR BUSINESS

Proactive Defense Strategies

Businesses that approach compliance, with HITRUST or otherwise, as one piece of the bigger picture ensure they remain compliant, while fully protecting their company, employees and customers in an economical way. Finding a partner that does both means better outcomes for your business.

Layered Approach to Defense

Focus on Human Factors – Employee Training!

Cyber Hygiene

View as Business Issue – not an IT issue

Remember – just b/c you outsource it doesn't mean you don't have responsibility for it

9

WHAT DO I LOOK FOR IN A PROVIDER?

- Ability to support your entire cybersecurity journey
- "DO-ers" / "implementers of operational cybersecurity
- Reputation – check their references
- Culture / values fit
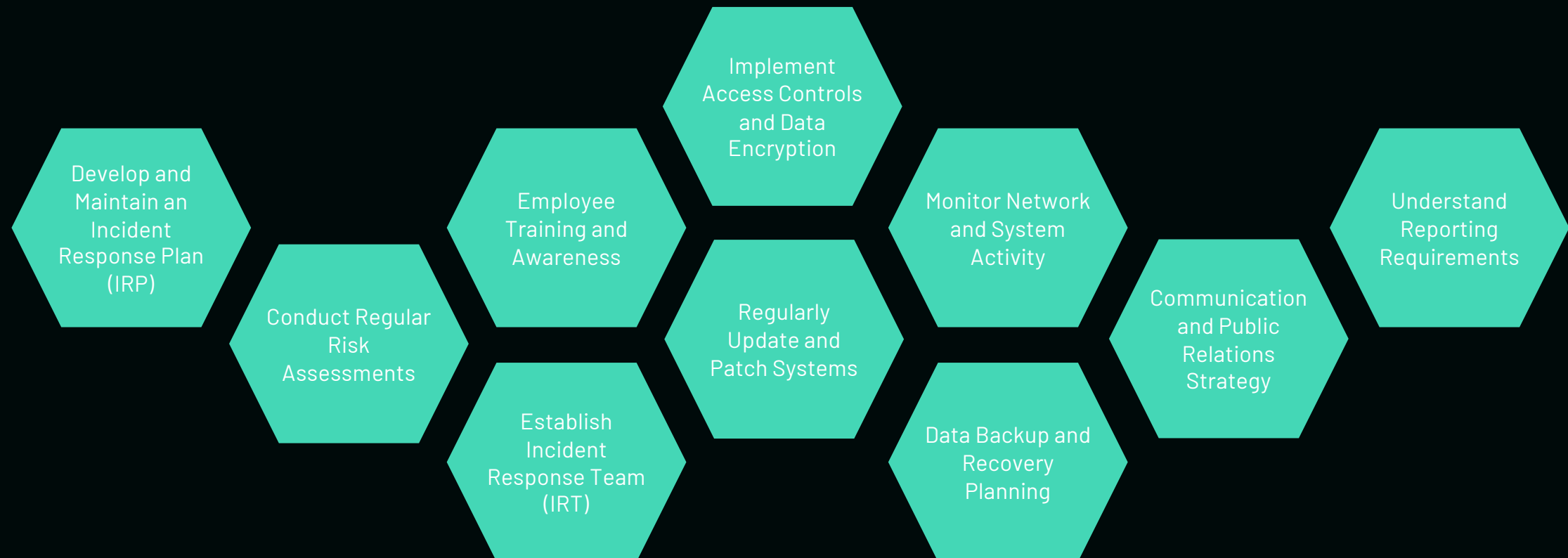- Transparent pricing – avoid hidden costs and fees

What about the costs?

$1,000s to $10,000s

How can I get buy-in to invest in cybersecurity?

Business Case, Productivity Gains, Risk Mitigation, Reduced Cyber Insurance Premiums,

10

CYBERSECURITY
INCIDENTS

Key steps to prepare for, respond to, and recover

Implement Access Controls and Data Encryption

Develop and Maintain an Incident Response Plan (IRP)

Employee Training and Awareness

Monitor Network and System Activity

Understand Reporting Requirements

Conduct Regular Risk Assessments

Regularly Update and Patch Systems

Communication and Public Relations Strategy

Establish Incident Response Team (IRT)

Data Backup and Recovery Planning

PANELIST Q&A

AUDIENCE Q&A

Use the Q&A function within Zoom to submit
your questions to our panelists.

THANK YOU FOR ATTENDING!

If you have further questions or would like additional information, feel free to contact Rod at **rod@usxcyber.com**.