

**NYSTEC**  
YOUR INDEPENDENT TECHNOLOGY ADVISOR

# Healthcare Risks and Security Best Practices


Presentation for:



**HCCA**<sup>TM</sup>  
Health Care Compliance  
Association

Advice  
Strategy  
Solutions  
Consulting

## Presenting Today

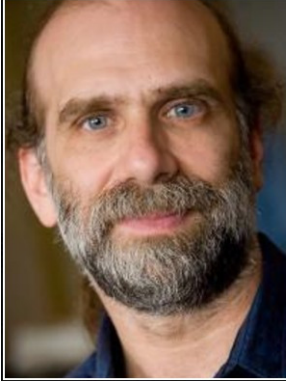



**JEFF PEREIRA**  
Principal Consultant  
Cell Phone: (646) 621-8050  
Email: [jpereira@nystec.com](mailto:jpereira@nystec.com)

<http://www.nystec.com/>  
<https://infosec.nystec.com/>

2

**Technology is the answer!**



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.


— Bruce Schneier —

AZ QUOTES


3

[www.schneier.com](http://www.schneier.com)

**Risk Defined**



**Risk** is a function of the likelihood of a given **threat** source exercising a particular potential **vulnerability** and the resulting **impact** of that adverse event on the organization.



4

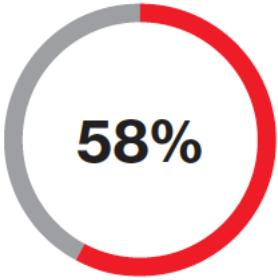
# Thinking about Healthcare Risk

- Threats
  - Criminal
  - Hacktivism
  - Insiders
- Vulnerabilities
  - Lack of Incident Response
  - Unpatched software
  - Weak authentication
  - Untrained workers
- Controls
  - System hardening
  - Patch management
  - Network segmentation



5

# Healthcare Risk Landscape



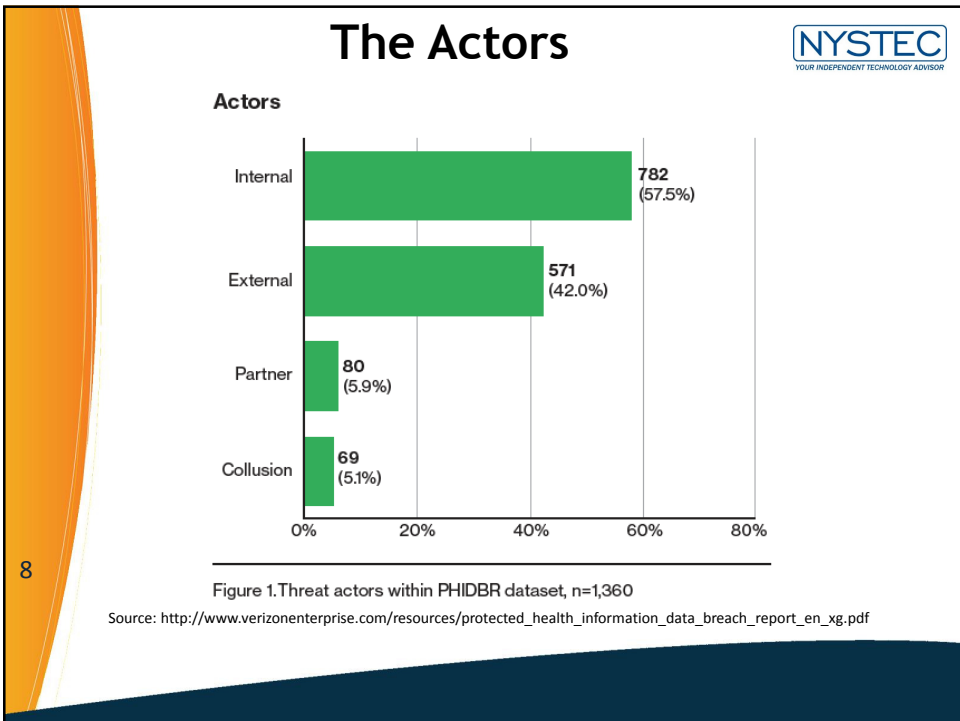
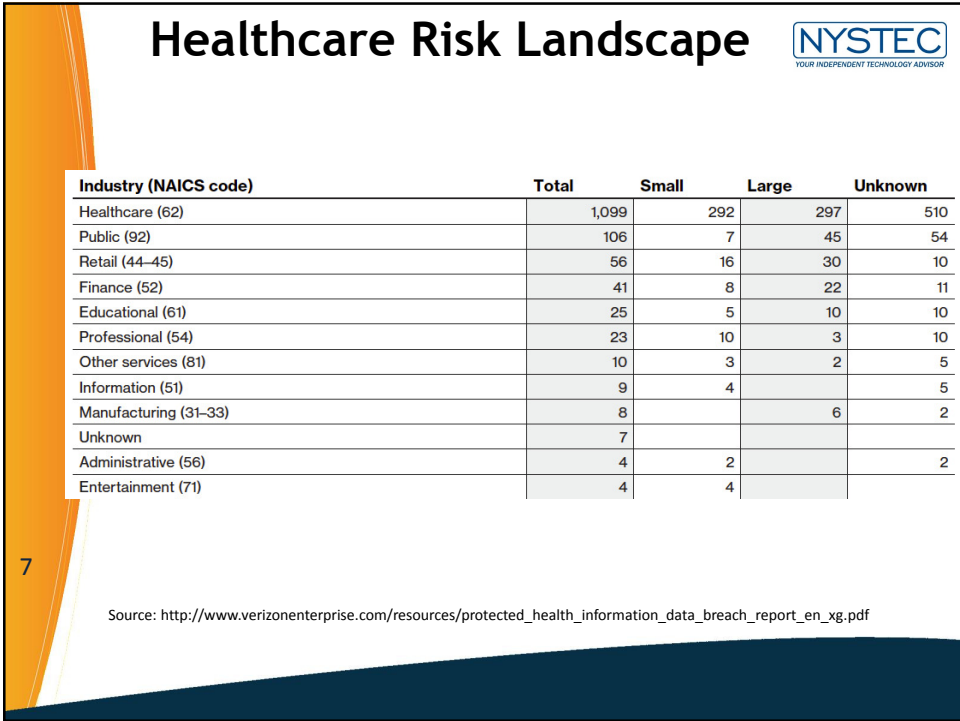
**58%**

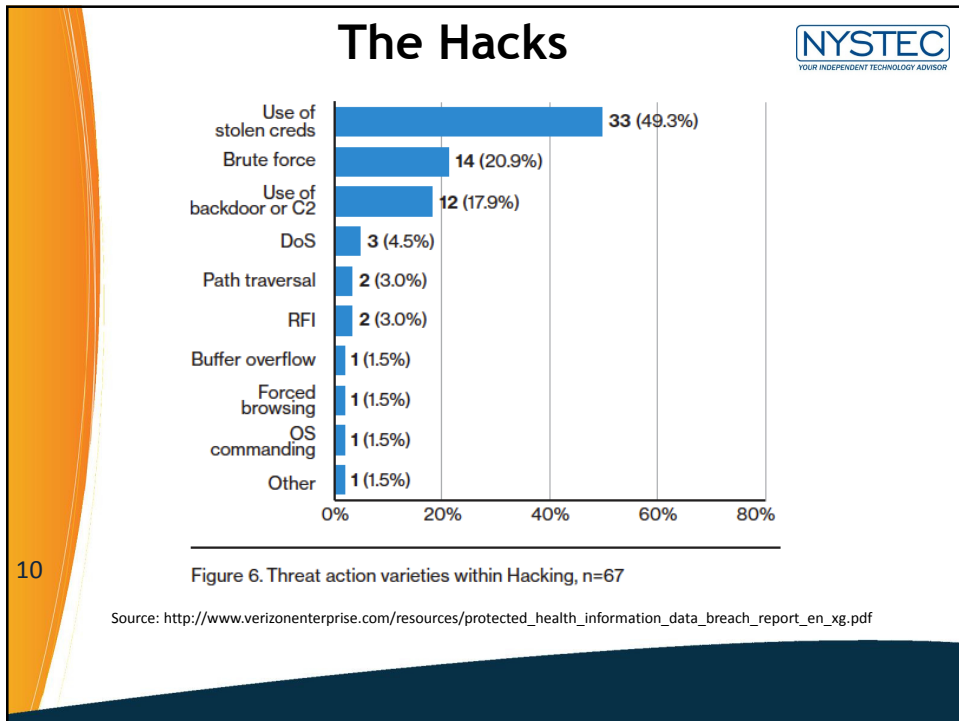
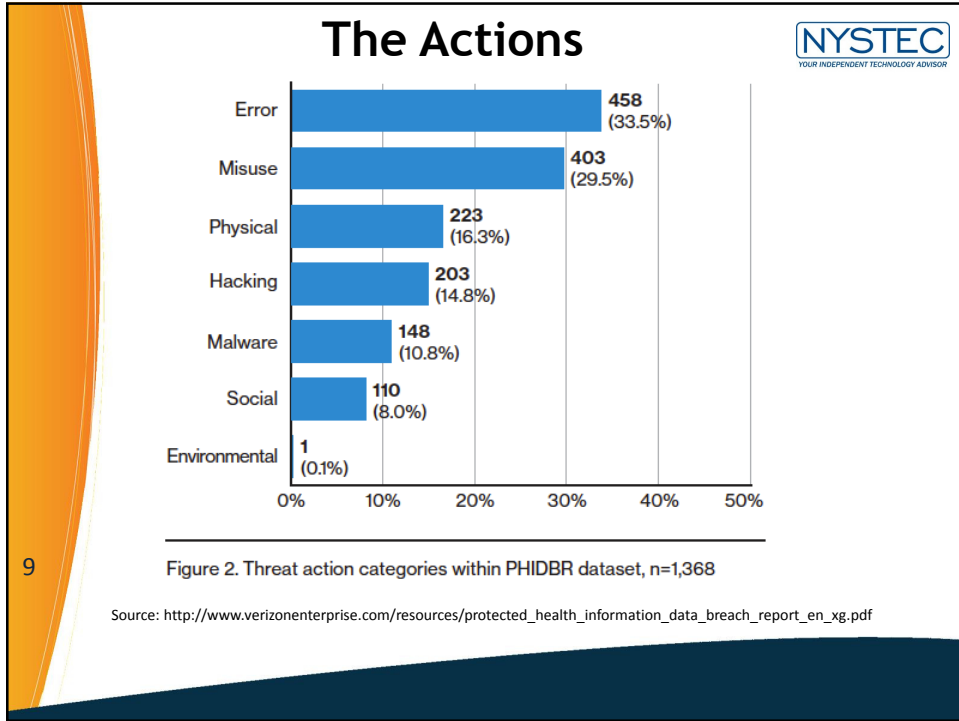
---

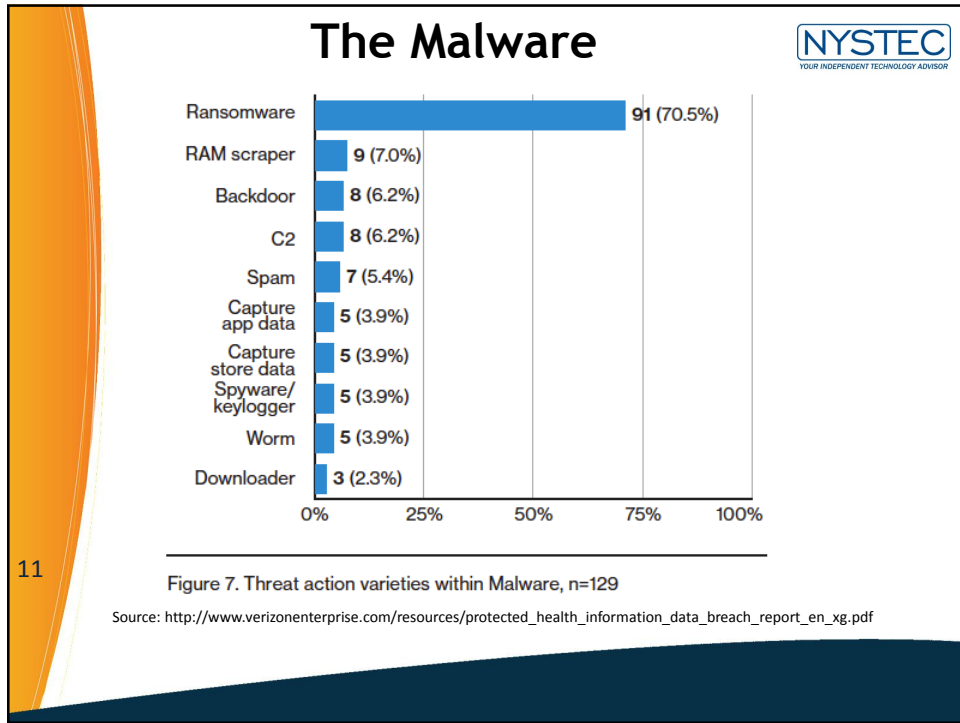
58% of incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization.

6

Source: [http://www.verizonenterprise.com/resources/protected\\_health\\_information\\_data\\_breach\\_report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf)







11

## The Results?

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
<input type="checkbox"/>	Banner Health	AZ	Healthcare Provider	362000	08/03/2016	Hacking/IT Incident	Network Server, Other
<input type="checkbox"/>	Newkirk Products, Inc.	NY	Business Associate	3466120	08/09/2016	Hacking/IT Incident	Network Server
<input type="checkbox"/>	Commonwealth Health Corporation	KY	Healthcare Provider	697800	03/01/2017	Theft	Other
<input type="checkbox"/>	Bon Secours Health System Incorporated	MD	Healthcare Provider	651971	08/12/2016	Unauthorized Access/Disclosure	Network Server
<input type="checkbox"/>	Peachtree Orthopaedic Clinic	GA	Healthcare Provider	531000	11/18/2016	Hacking/IT Incident	Network Server
<input type="checkbox"/>	Alway Oxygen, Inc.	MI	Healthcare Provider	500000	06/16/2017	Hacking/IT Incident	Network Server
<input type="checkbox"/>	California Correctional Health Care Services	CA	Healthcare Provider	400000	05/15/2016	Theft	Laptop
<input type="checkbox"/>	Women's Health Care Group of PA, LLC	PA	Healthcare Provider	300000	07/15/2017	Hacking/IT Incident	Desktop Computer, Network Server
<input type="checkbox"/>	Oklahoma State University Center for Health Sciences	OK	Healthcare Provider	279865	01/05/2018	Hacking/IT Incident	Network Server
<input type="checkbox"/>	Urology Austin, PLLC	TX	Healthcare Provider	279663	03/22/2017	Hacking/IT Incident	Network Server
<input type="checkbox"/>	Pacific Alliance Medical Center	CA	Healthcare Provider	266123	08/10/2017	Hacking/IT Incident	Network Server
<input type="checkbox"/>	Athens Orthopedic Clinic, P.A.	GA	Healthcare Provider	201000	07/29/2016	Unauthorized Access/Disclosure	Electronic Medical Record
<input type="checkbox"/>	Peachtree Neurological Clinic, P.C.	GA	Healthcare Provider	176295	07/07/2017	Hacking/IT Incident	Network Server
<input type="checkbox"/>	St. Peter's Ambulatory Surgery Center LLC - d/b/a St. Peter's Surgery & Endoscopy Center	NY	Healthcare Provider	134512	02/28/2018	Hacking/IT Incident	Network Server
<input type="checkbox"/>	Arkansas Oral & Facial Surgery Center	AR	Healthcare Provider	128000	09/24/2017	Hacking/IT Incident	Network Server

[https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

1

# Threats



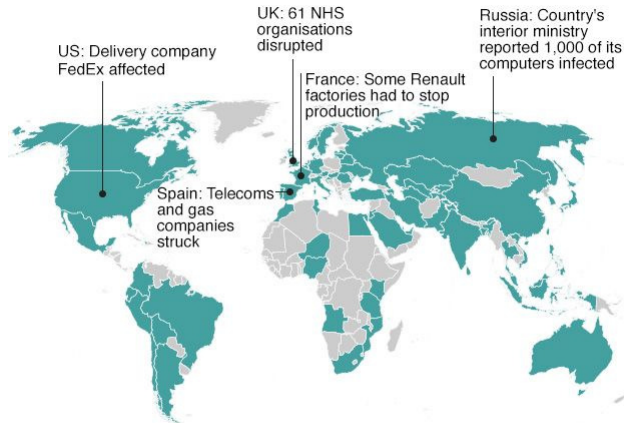
13

Source: krebsonsecurity.com

# Threats



## Countries hit in initial hours of cyber-attack



14

\*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team



**NYSTEC**  
YOUR INDEPENDENT TECHNOLOGY ADVISOR

## Threats

A surgical center affiliated with St. Peter's Hospital has been hit by the second-largest computer breach of patient records in New York state since 2016. Timesunion.com







**Sheriffs warn of hackers after upstate attack**  
Thedailystar.com





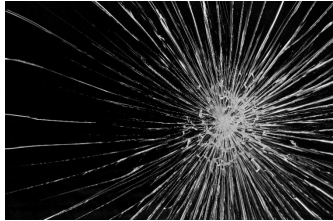


15

**NYSTEC**  
YOUR INDEPENDENT TECHNOLOGY ADVISOR

## Impact of a Breach

- **Financial**
  - Revenue loss
  - Cost of breach \$154-\$158/record (2016 Ponemon Institute\*)
  - Credit monitoring (~\$40/person per year)
  - HIPAA penalty up to \$1.5M/year
  - Cost of litigation and mitigation
- **Other**
  - **Public safety**
  - Productivity loss
  - Legal/regulatory/contract issues
  - Damage to reputation
  - **Loss of Life**



16

\* <https://securityintelligence.com/media/2016-cost-data-breach-study/>



## Why is Healthcare such a target?

- IOT and Medical Devices
- Value of health data
- Low barriers to market entry
- Critical services provided
- Late adopters of technology
- HIPAA not enough



17

## Healthcare Security



**Best Practices**

18

## #1 Incident Response

**NYSTEC**  
YOUR INDEPENDENT TECHNOLOGY ADVISOR

- Are you ready?
- Incident Response Plan
- Tabletop exercises
- Expert help when needed
- Considerations
- No longer if, but when

19

## #2 Patch, Patch, Patch

**NYSTEC**  
YOUR INDEPENDENT TECHNOLOGY ADVISOR

- Remove the low hanging fruit
- Make it part of your IT culture
- Updates to software
- Some outages is a small price to pay
- Software & hardware inventories

20

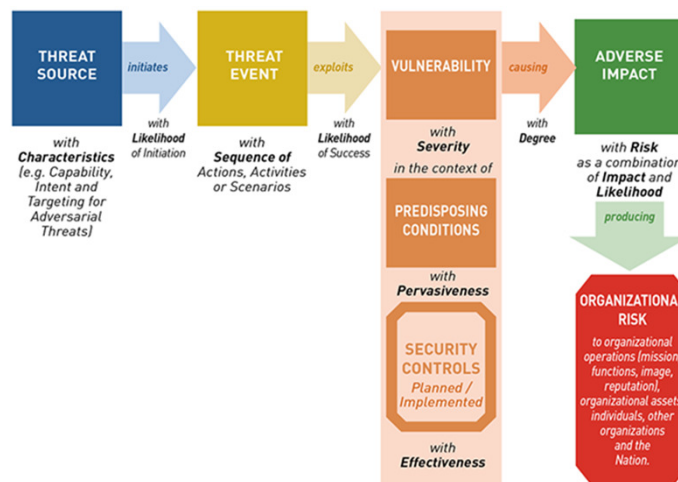
### #3 Vulnerability Assessment

- External scanning
- Internal scanning
- Web Application Testing
- Authenticated scanning
- Penetration Testing
- Social Engineering
- Physical Security



21

### #4 Conduct A Risk Assessment



22

source: <https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1>

## #5 Security Awareness Training



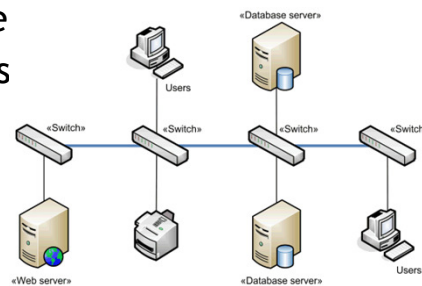
- Emails
- Lunch and Learns
- Posters
- Phishing Awareness
- Regular staff awareness training
- Screen savers
- Make it part of your corporate culture

23

## #6 Network Segmentation



- Isolate critical assets
- Layers of defense
- Security zones
- Reduce attack space
- Cloud considerations



24

## #7 Critical Data Handling



- Data Classification
- Asset Inventory
- Isolation of sensitive data
- Backups, backups, backups
- Think before you expose your data

25

## #8 Multifactor Authentication



- Passwords are dead
- Credential theft is too common
- MFA is effective and worth the cost
- Mandatory for privileged access
- Recommended for all



26

# #9 Cloud/Hosted Services

- Considerations
- Benefits
- Risks



27

# #10 Align with CIS Top 20\*

<b>1</b> Inventory of Authorized and Unauthorized Devices	<b>11</b> Secure Configurations for Network Devices
<b>2</b> Inventory of Authorized and Unauthorized Software	<b>12</b> Boundary Defense
<b>3</b> Secure Configurations for Hardware and Software	<b>13</b> Data Protection
<b>4</b> Continuous Vulnerability Assessment and Remediation	<b>14</b> Controlled Access Based on the Need to Know
<b>5</b> Controlled Use of Administrative Privileges	<b>15</b> Wireless Access Control
<b>6</b> Maintenance, Monitoring and Analysis of Audit Logs	<b>16</b> Account Monitoring and Control
<b>7</b> Email and Web Browser Protections	<b>17</b> Security Skills Assessment and Appropriate Training to Fill Gaps
<b>8</b> Malware Defenses	<b>18</b> Application Software Security
<b>9</b> Limitation and Control of Network Ports	<b>19</b> Incident Response and Management
<b>10</b> Data Recovery Capability	<b>20</b> Penetration Tests and Red Team Exercises



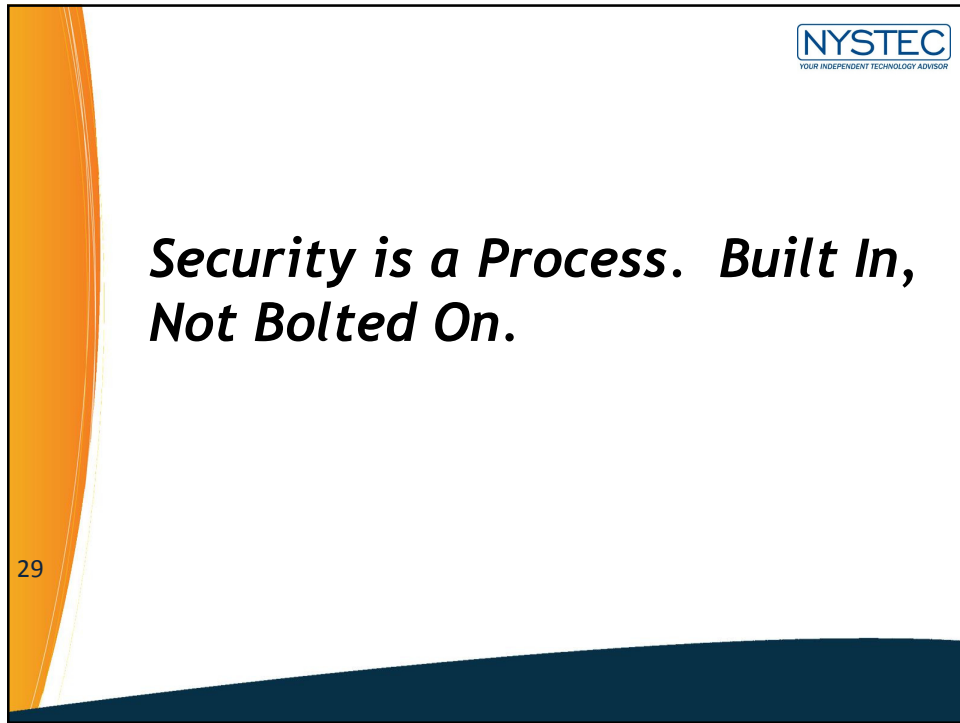
\* <https://www.cisecurity.org/critical-controls.cfm>

28

NYSTEC  
YOUR INDEPENDENT TECHNOLOGY ADVISOR


***Security is a Process. Built In,  
Not Bolted On.***

29

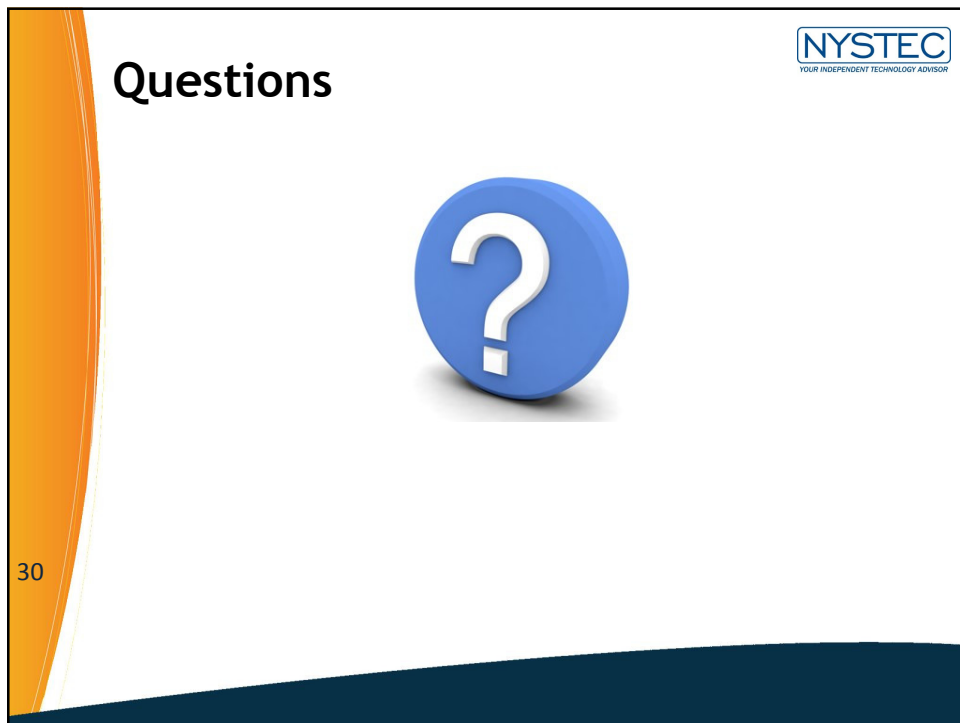
This slide features a white background with a dark blue wave at the bottom and an orange curved shape on the left. The NYSTEC logo is in the top right. The main text is centered and italicized.

NYSTEC  
YOUR INDEPENDENT TECHNOLOGY ADVISOR

**Questions**



30

This slide features a white background with a dark blue wave at the bottom and an orange curved shape on the left. The NYSTEC logo is in the top right. The word "Questions" is in the top left. A large 3D blue question mark icon is centered on the slide.