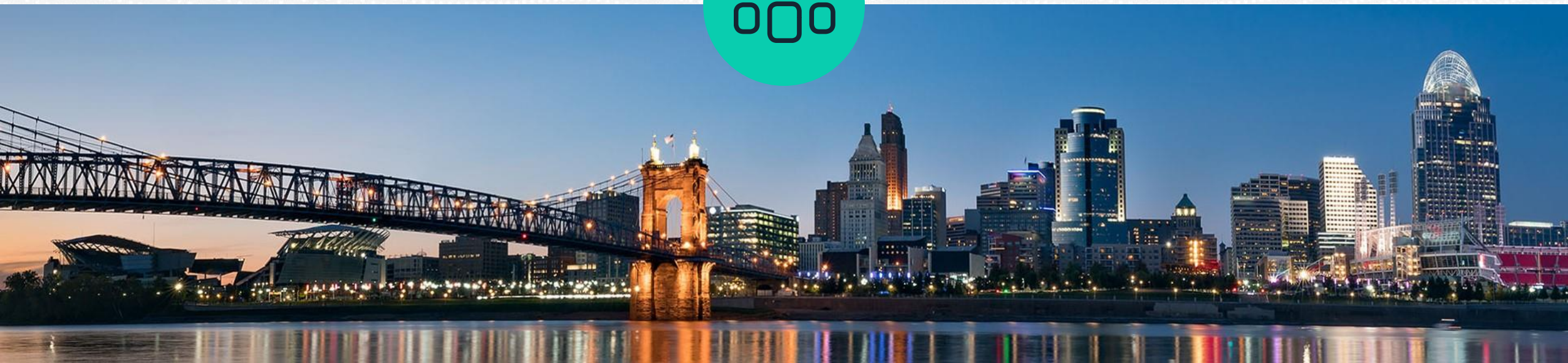
Best Practices for Defeating Ransomware

A CBTS Security Webinar for SMBs

/usr/bin/whoami

- Justin Hall
  - Cincinnati native
  - Husband & dad
  - 20+ years in IT
  - 14+ years in security

- Director of Security Consulting at CBTS
- GCIH Gold / GCFA / GPEN
- University of Cincinnati College of Business alumnus
- linkedin.com/in/justinwhall



The CBTS Security Practice

Solution Design & Recommendation

- Secure network design, product selection & evaluation
- Over 70 security vendor partnerships

Security Assessments & Penetration Testing

- Standards-based assessments performed by industry veterans
- Customized findings reports with prioritized recommendations

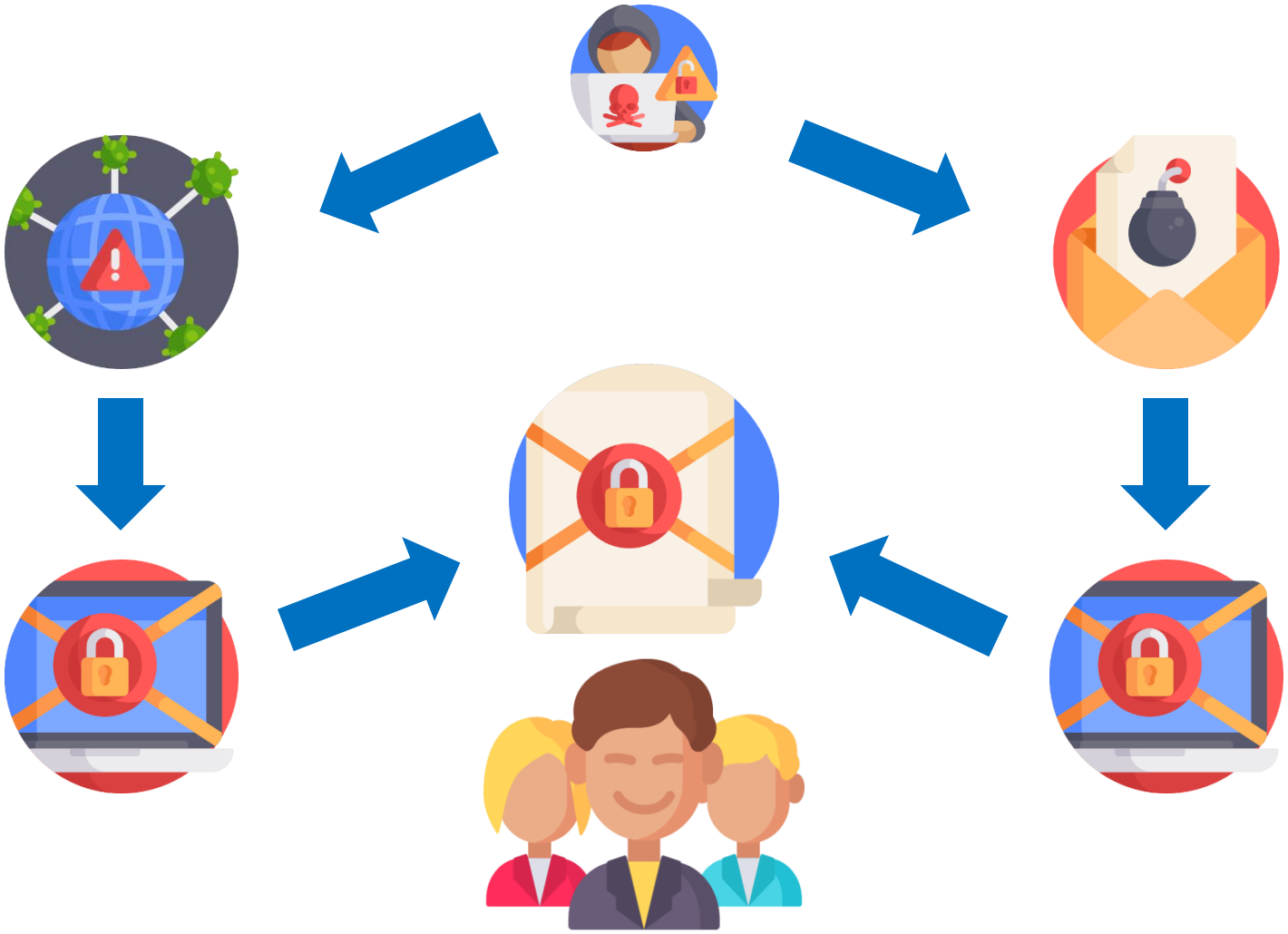
Strategic Staffing & Recruiting

- Staff augmentation, contract, contract-to-hire
- Personal recruiter finds and vets resources that meet specific needs


Cleveland Airport Suffers Ransomware Attack
Baltimore ransomware attack will cost the city over $18 million
City residents are still facing issues.
Key Biscayn
June 2019 --
joining Riviera Beach & Lake City.

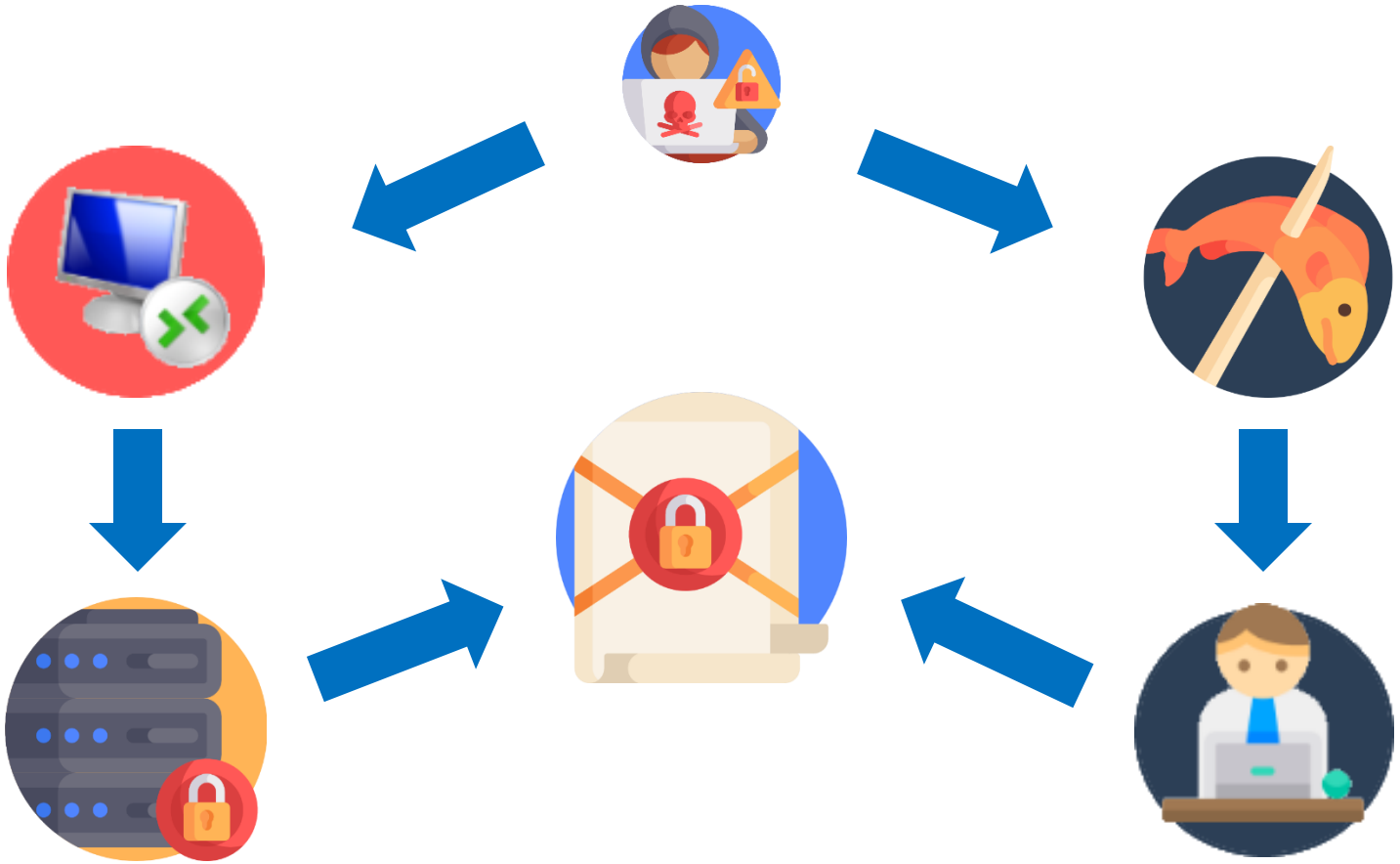
Opportunistic Ransomware Attacks

cbts



Targeted Ransomware Attacks

cbts



Root Causes of Ransomware Issues

cbts

Gaps in security controls that allow successful attacks

- Failure to effectively **filter web and email traffic**
  - Malware is allowed into a user's hands
- Failure to **stop malicious code from executing** on assets
  - Malware is allowed to execute
- Failure to **restrict access to critical data** and applications
  - Malware is allowed to overwrite data
- Failure to **train users to recognize and report** social engineering and phishing
  - Users provide attackers with access to the environment
- Lack of **visibility into suspicious or malicious activity** in computing environment
  - Malware is allowed to propogate
- Missing **incident response** capability
  - Slow, inefficient, ineffective containment, eradication and remediation

1 in 412

Email messages are malicious

1 in 10

URLs accessed by clients are malicious

5200

IoT / Smart devices experience 5200 attacks per month

New in 2018

246M Malware variants

187M Ransomware variants

2300 Mobile malware variants

Regulatory Compliance is Insufficient

Confusing Product Landscape

New Threats and Vulnerabilities

Skills and Resources Gap

Critical Security Controls for Ransomware Defense

The CIS Critical Security Controls v7.1

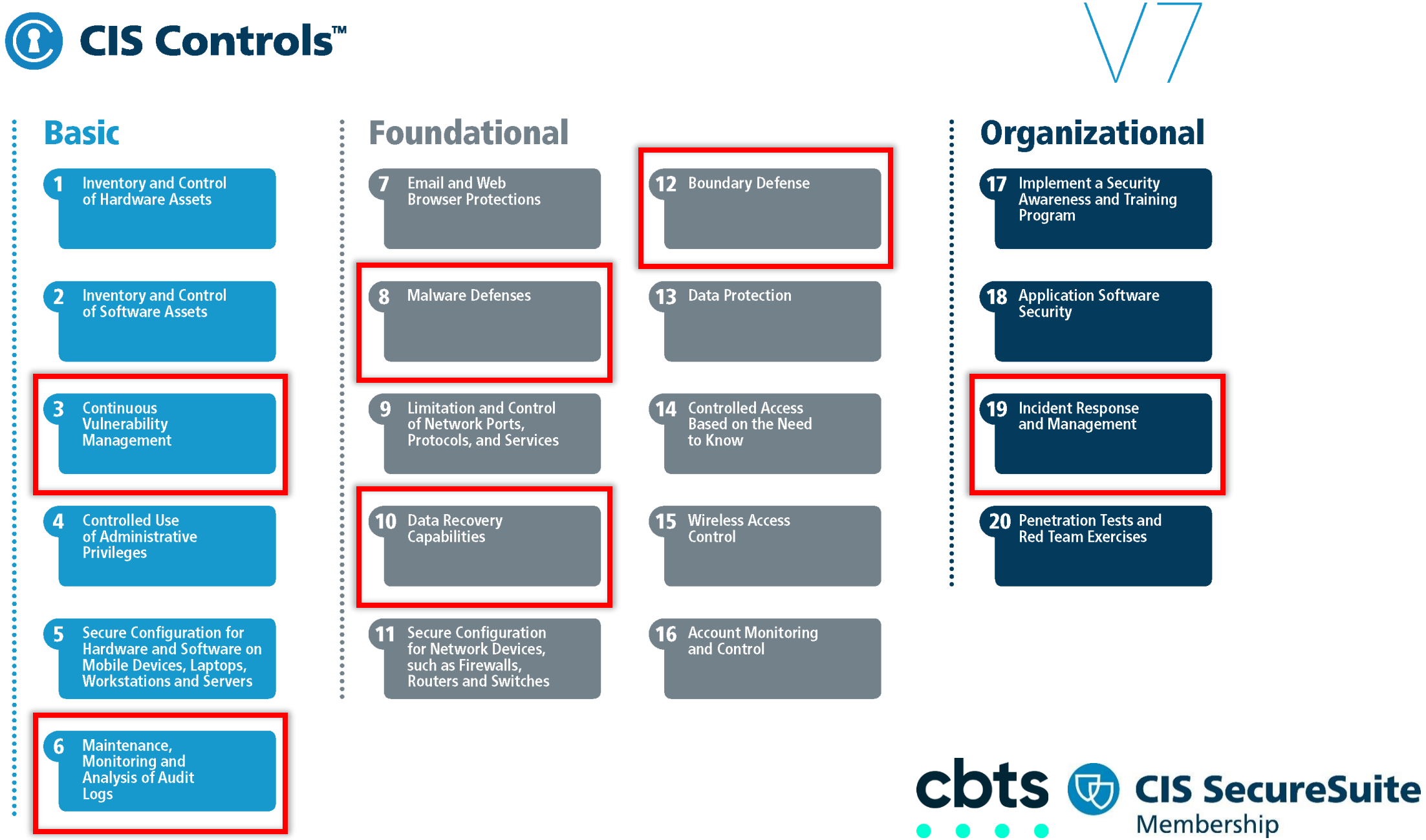
cbts

A **free resource** published by the CIS Center for Internet Security®

- Aligns with several **popular security frameworks**, including:
  - NIST Cybersecurity Framework & 800-53
  - ISO27000
  - PCI-DSS
  - HIPAA Security Rule
  - NERC CIP
  - FISMA

- Contains **20 control categories**
  - Basic / Foundational / Organizational
  - Each category has several individual control requirements

- Controls broken up into three **Implementation Groups**
  - Helps organizations of different sizes select controls to deploy


CIS Controls™
V7
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols, and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises
cbts
CIS SecureSuite Membership

About CSC Implementation Group 1

- An IG1 organization is **small to medium-sized** with **limited IT and cybersecurity expertise** to dedicate toward protecting IT assets and personnel.
- The principal concern of these organizations is to **keep the business operational** as they have a limited tolerance for downtime. The **sensitivity of the data that they are trying to protect is low** and principally surrounds employee and financial information. However, there may be some small to medium-sized organizations that are responsible for protecting sensitive data and, therefore, will fall into a higher Group.
- Sub-Controls selected for IG1 should be implementable with **limited cybersecurity expertise** and **aimed to thwart general, non-targeted attacks**. These Sub-Controls will also typically be designed to work in conjunction with **small or home office commercial-off-the-Shelf (COTS) hardware and software**.

About CSC Implementation Group 2

cbts

CIS.

- An IG2 organization **employs individuals responsible for managing and protecting IT infrastructure**. These organizations support multiple departments with differing risk profiles based on job function and mission. Small organizational units may have regulatory compliance burdens.
- IG2 organizations often **store and process sensitive client or company information** and can withstand short interruptions of service. A major concern is **loss of public confidence** if a breach occurs.
- Sub-Controls selected for IG2 **help security teams cope with increased operational complexity**. Some Sub-Controls will **depend on enterprise-grade technology** and specialized expertise to properly install and configure.

Control #3: Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Implementation Group 1

- Deploy Automated **Operating System Patch Management** Tools
- Deploy Automated **Software Patch Management** Tools

Implementation Group 2

- Run **Automated Vulnerability Scanning** Tools
- Perform **Authenticated** Vulnerability Scanning
- **Protect** Dedicated Assessment Accounts
- Compare **Back-to-Back** Vulnerability Scans
- Utilize a **Risk-Rating Process**

Control #6: Maintenance, Monitoring, & Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Implementation Group 1

- Activate **Audit Logging**

Implementation Group 2

- Utilize three **synchronized** time sources
- Enable **detailed** logging
- Ensure **adequate storage** for logs
- **Central** log management
- Deploy **SIEM** or Log Analytics Tools
- Regularly **review** logs

Control #8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Implementation Group 1

- Ensure Anti-Malware Software and Signatures Are **Updated**
- Configure Anti-Malware Scanning of **Removable Media**
- Configure Devices to **Not Auto-Run** Content

Implementation Group 2

- Utilize **Centrally Managed** Anti-Malware Software
- Enable Operating System **Anti-Exploitation** Features, and Deploy Anti- Exploit Technologies
- **Centralize** Anti-Malware Logging
- Enable **DNS Query** Logging
- Enable **Command-Line** Audit Logging

Control #10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Implementation Group 1

- Ensure **Regular Automated** Backups
- Perform **Complete System** Backups
- **Protect** Backups
- Ensure All Backups Have **at Least One Offline** Backup Destination

Implementation Group 2

- **Test Data** on Backup Media

Control #12: Boundary Defense

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Implementation Group 1

- Maintain an **Inventory of Network Boundaries**
- Deny Communication Over **Unauthorized Ports**

Implementation Group 2

- **Scan for Unauthorized Connections** Across Trusted Network Boundaries
- Deny Communications With **Known Malicious IP Addresses**
- Configure Monitoring Systems to **Record Network Packets**
- Deploy Network-Based **IDS Sensors**
- Deploy **NetFlow Collection** on Networking Boundary Devices
- Require All Remote Logins to Use **Multi- Factor Authentication**

Control #19: Incident Response & Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Implementation Group 1

- Document Incident Response **Procedures**
- Designate **Management Personnel** to Support Incident Handling
- Maintain **Contact Information** For Reporting Security Incidents
- Publish Information Regarding **Reporting Computer Anomalies and Incidents**

Implementation Group 2

- Assign **Job Titles and Duties** for Incident Response
- Devise **Organization-wide Standards** For Reporting Incidents
- Conduct Periodic **Incident Scenario Sessions** for Personnel

Addressing Your Control Gaps

cbts

What should we fix? What solutions should we use? How do we prioritize?

- Your security program's **formal risk management process** should see control gaps as risks
  - Launch an initiative to assess your control gaps
  - Develop a remediation strategy to address gaps
  - Prioritize remediation actions according to threat landscape, past issues, business requirements, available resources and budget
  - Execute strategy – deploy controls, measure effectiveness
- **Regularly review** control strategy to ensure alignment with risk posture
- **Solicit feedback** from third parties and experts
  - Industry peers – possibly even competitors
  - Local security community
  - Available experts

The CBTS Security Architecture Assessment

CBTS Security Consulting experts work with you to **discover control gaps**, develop a **remediation strategy**, and craft a **roadmap** to execute it.

- **2-3 week** hands-on consulting engagement
- Based on **CIS Controls v7.1**
- Review of controls, defenses, policies, processes
- Hardening review of **gold images** for servers & workstations
- **Custom findings report** with detailed, prioritized recommendations
- **Executive summary** + presentation of results to leadership

Case Study – Healthcare Services Firm

- Local healthcare lab & testing firm
- Founded in 1994
- Privately held

Challenge

- The customer had a growing business and some IT staff, but no dedicated security practitioners or leadership. Faced with a growing risk profile, they needed a strategy to protect the PHI and ePHI of their customers and to be HIPAA compliant.

Solution

- CBTS performed a Security Architecture Assessment, reviewing their adherence to the CIS Critical Controls.
- The customer's server and workstation gold images were analyzed to find configuration gaps
- Placement of security controls and network design and configuration were examined by CBTS consultants

Result

- A three-phase, multi-year roadmap of security projects was provided
- A detailed, handwritten findings report outlined the issues and listed prioritized recommendations
- A post-assessment review helped talk the CIO and staff through the next steps to mature the security program

How to Engage Us

Justin Hall - Director, Security Consulting
justin.hall@cbts.com | 513.252.6011

Tim Linder - Director, Security Sales
tim.linder@cbts.com | 513.706.5270

Eric Bell – Security Specialist, North/East
eric.bell@cbts.com | 614.329.6674

Joe Graue – Security Specialist, South
joseph.graue@cbts.com | 859.835.2860

Eric Vibberts – Security Specialist, Central/West
eric.vibberts@cbts.com | 513.207.1404

Questions?

justin.hall@cbts.com

@justinhall

linkedin.com/in/justinwhall

cbts