NCSHA

HFAs AT THE CENTER

AUSTIN 2018 ANNUAL CONFERENCE & SHOWPLACE

# Cybersecurity: Protecting Your Clients and Organization

October 15, 2018

# Presenters

## Texas Department of Housing and Community Affairs

Curtis Howe, Director of Information Systems

Jordan Genung, CISSP, Information Security Officer

Larry Mercadel, Network Administrator

## New Hampshire Housing Finance Authority

David Hebert, Managing Director of Information Technology

## WP Engine

Brent Stackhouse, Director of Security

# Session Overview

1. Three presentations and Q&A to provide real, practical help in assessing and improving your organization's information security program

2. Information for everyone (business and technical)

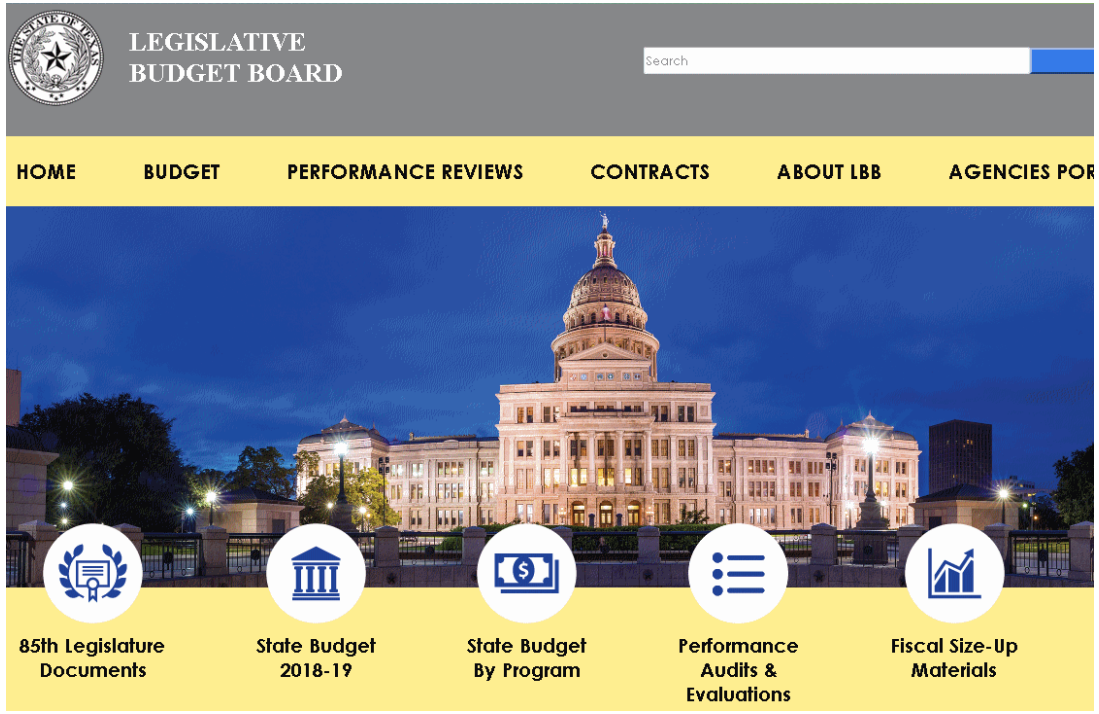
3. Cybersecurity management, planning, and budgeting

# TDHCA Presentation Agenda

1. Planning and budgeting, with Texas examples
2. Texas Cybersecurity Framework
3. Threat landscape
4. Security considerations

# 1. Cybersecurity Planning and Budgeting

- Think of information security as a critical service to your customers, not just as costs and controls
- Legislators, executive management, and customers expect you to budget time and money for security
- In Texas, special procedures for cybersecurity components of agency appropriations requests highlight the emphasis on protecting customer data



# 2. Texas Cybersecurity Framework

- Based on NIST CSF and FISMA
- Components:
  - Texas Administrative Code (TAC) Chapter §202
  - Controls Standards Catalog (based on NIST SP800-53)
  - Biennial Agency Security Plan (based on NIST CSF)
- Utilized by Texas state agencies and higher education
- Texas Department of Information Resources website:
  www.dir.texas.gov > Resources > Information Security

# 3. Threat Landscape

**Threats**

- Ransomware
- Data breaches
- Phishing
- Insider threats

**Causes Of Compromise**

- Lack of basic cyber hygiene
- Lack of patching/misconfiguration
- Credential theft
- Lack of monitoring, training, and awareness

**HFAs have an important responsibility to protect customer data**

# 4. Security Considerations

- Security governance
- Best practice frameworks
- Risk management
- Attack surface considerations
- Policies and procedures
- Foundational practices
- BCP/DRP/IRP
- Security awareness training

# Security Governance

- Executive support
- Resource allocation
- Align security with business requirements

**Lack of security governance**

# Best Practice Frameworks

- Texas Cybersecurity Framework
- NIST Cybersecurity Framework
- ISO 27001/27002
- **Center for Internet Security - MS-ISAC** Critical Security Controls

| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| | Supply Chain Risk Management | ID.SC |
| Protect | Identity Management and Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

**NIST Cybersecurity Framework**

# Risk Management

- Assessment, prioritization, and response to risk

- Considerations:
  - Do you have an inventory of systems?
  - Do you know which systems hold confidential or sensitive information?
  - Which systems are Internet facing and what services are running?

# Attack Surface Considerations

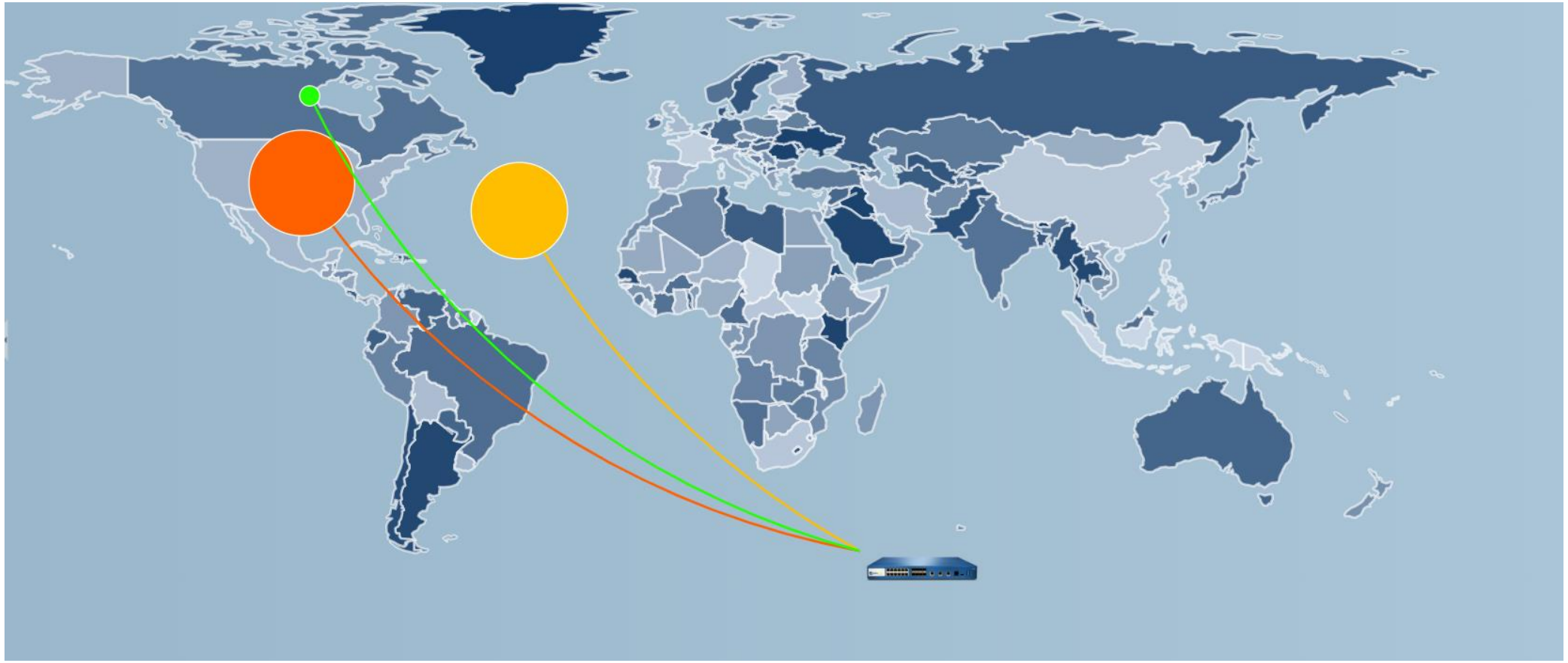
- Reduce attack surface
  - Internet facing systems
  - Domain and IP blocking
  - Country blocking

- DNS Blocking: Quad9
  https://www.globalcyberalliance.org/quad9/

- Comprehensive coverage: Web, email, and endpoint protection

# Attack Surface – Before Country Blocking

# Attack Surface – After Country Blocking

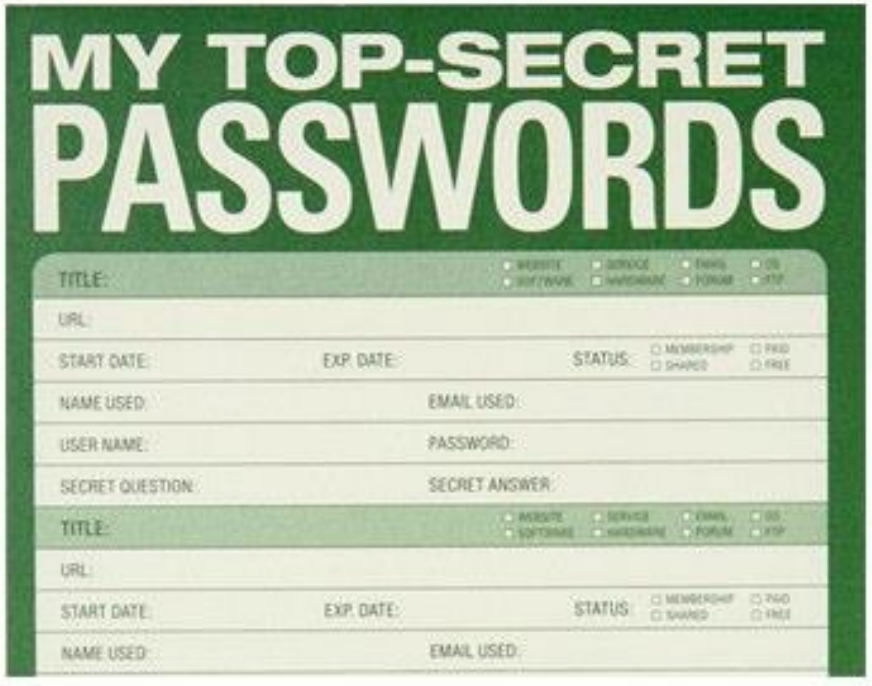


# Policies and Procedures

- Need to have them
- Need to enforce them
- Data classification is important!

# Foundational Practices

- Inventory management
- Patch and vulnerability management
- Configuration and change management
- Credential management



# BCP/DRP/IRP

- Business continuity planning
- Disaster recovery planning
- Incident response planning

# Security Awareness Training

- Fairly inexpensive….unless you don't do it!!

- Considerations:
  - In person training
  - Computer based training
  - Monthly newsletters
  - Simulated phishing exercises