2019 Boston

ANNUAL CONFERENCE & SHOWPLACE

What HFAs and Their Partners Need to Know About Cybersecurity

Metrics and Measures

NCSHA

Metrics and Measures

- Del Collins
- Director of Information Technology
- South Carolina Housing Finance and Development Authority
- (803) 896-8725
- del.collins@schousing.com
- www.schousing.com

Chronology of Data Breaches

Chronology of Data Breaches Search

- Breach Type: CARD, HACK, INSD, PHYS, PORT, STAT, DISC, UNKN
- Organization Type: BSF, BSO, BSR, EDU, GOV, MED, NGO, UNKN
- Year(s) of Breach: 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009, 2008, 2007, 2006, 2005
- Company or Organization: all
- Breaches made public fitting this criteria: 8,994
- **Records total: 10,400,334,031**

Source privacyrights.org (The data breach file was so large I could not download it from their servers)

Vulnerability Search (NIST)

- Search Parameters: Vulnerabilities: All, Date Range: All, CVSS Metrics: All
- **Records total: There are 122,655 matching records.**

Source National Institute of Standards and Technology (nist.gov)

Vulnerability Search (CERT/CC)

- Search Parameters: Vulnerabilities: All, Date Range: All (2000-2019)
- **Records total: 3480 Results**

Source Computer Emergency Response Team Coordination Center (sei.cmu.edu/about/divisions/cert/)

Security Technical Implementation Guides (STIG Library)

- **590 STIG Topics**

Source US Dept of Defense Cyber Exchange (Public) (https://public.cyber.mil/)

Only You Can Answer The Question

- Industry wide there exist a plethora of suggestions and recommendations for metrics and the data that should be collected with little effort to correlate or validate these measures to actual, practical infrastructure operations or to determine their effect on day-to-day operations of an organization

- Common Vulnerability Scoring System (CVSS) Training: https://learning.first.org/dashboard

Glancing at Metrics and Measures

Interesting Statistics:

- Looking for what key performance indicators cybersecurity professionals recommended?
- Looking for what executive level professionals thought were most important?
- Looking for what new IT graduates thought were most important?
- Looking for where financial officers thought the budget was being spent?

Sources: SourceFirst, LinkedIn, IBM, Cisco, Brookings Institute, Forbes, WeForum, MIT, Harvard, SANS, FTC, RSAConference, Northrup Grumman, Microsoft, NIST, Cyber Defense Magazine, Norton, Inside Cyber Security, International Trade Regulation and Cybersecurity, Wall Street Journal, CSO Online, Cambridge, Carnegie Mellon Institute, CERT/CC, Washington Post, Security Industry Association, United Nations Economic Commission Trade Program

Cybersecurity Professionals

- Polled 100's "Professionals" (Articles, Interviews, Blogs, Websites)
  1. Incidents, 33%
     1. Malware (Adware, Browser Jacking, Cryptojacking, Fake Security, Ransomeware, Spyware, Viruses, Bots, Botnets, Keyloggers, Phishing, Spearphishing, Rootkits, Trojans and Worms) <1/3
        1. Phishing
  2. Personnel 11%
     1. Training >1/2
  3. Patch Latency, 10%
  4. Vulnerability Identification, 8%
  5. Budget, Monitoring and Compliance all tied for 5th place. 6% ea.
  6. Policies 4%
  7. Project Completion, Disaster Recovery, # Assets Protected, Audit 3% ea.
  8. 3rd Party Risks, Inventory, Upgrade Latency, Password Policy 1% ea.

What do Others Think?

- Executives (What's the most critical component of your cybersecurity profile?):
    - Phishing Protection
- New IT Security (What are you looking for in a company recruitment program?)
    - Legal Requirements
    - Investment
    - # of Assets Covered
- Financial Officers (Where do they think the $$$ is being spent?)
    - Security Portfolio Tools
    - Backups
    - Malware Protection
    - Consulting (To install tools correctly)
    - Incident Response

What are Hackers Using For Metrics?

- Budget: How much targets are spending on cybersecurity?
- Team: How big and experienced is the cybersecurity team they are up against?
- % Assets Protected: How much of the target infrastructure is protected?
- Patch Latency: Are scans showing patching latency?
- Password Policy: Probing with default passwords success?

The More Things Change The More Things Stay The Same.

Source Cisco Oct 2018

Relative Scope and Scale

Source TechRepublic Feb 2018

Where Do You Start?

- Policies and Compliance Monitoring
- Data Classification and Controls
- Business Impact Analysis
- Business Continuity Policy and Planning
- Budget

- Incident Monitoring and Response Strategy
- Education
- Control Identification and Review
- Vulnerability Assessments
- Penetration Testing
- Common Vulnerability Scoring

Hacker Price Guide

- **Social Security number**: $1
- **Credit or debit card (credit cards are more popular)**: $5-$110
  - **With CVV number**: $5
  - **With bank info**: $15
  - **Fullz info**: $30*
- **Online payment services login info (e.g. Paypal)**: $20-$200
- **Loyalty accounts**: $20
- **Subscription services**: $1-$10
- **Diplomas**: $100-$400
- **Driver's license**: $20
- **Passports (US)**: $1000-$2000
- **Medical records**: $1-$1000**
- **General non-Financial Institution logins**: $1

*A bundle of information that includes: name, SSN, birth date, account numbers and other data.

**Depends on how complete they are as well as if its a single record or an entire database.

Source Experian Oct 2017