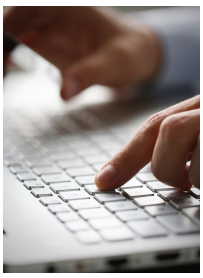
CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

BUSINESS DEFENSIVE CYBERSECURITY CHEAT SHEET

① Require Strong Credentials



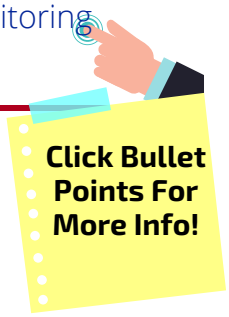
74% Of Data Breaches Start With Privileged Credential Abuse. Weak credentialing habits means that many fraud schemes don't require any malware.

- Require different email addresses for different sites
- Require uniquely different credentials for every login
- Tie Human resources to IT - so that IT is informed of all job changes access requirements
- Centralized Repository of corporate data, tools and logs
- Employ the Principal of Least Privilege
- Tune System to Automatically to remove employees credentials when they leave company
- Require Network credentials for sharing files

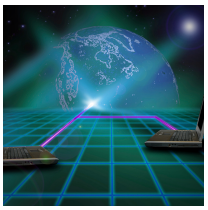
② Control and Monitor Empoyee Activity

Employee Monitoring is the act of employers surveying employee activity through different surveillance methods. Organizations engage in employee monitoring for different reasons such as to track performance, to avoid legal liability, to protect trade secrets, and to address other security concerns.

- The 2019 Clear and Complete Guide to Employee Monitoring
- What is Employee Monitoring Software?



③ Know Your Network



A network connects computers, mobile phones, peripherals, and even IoT devices. Switches, routers, and wireless access points are the essential networking basics. Through them, devices connected to your network can communicate with one another and with other networks, like the Internet.

- 2019 How-to Guide: Small Office Network Setup
- Basic Networking Concepts- Beginners Guide

④ Download and Install Patches and Updates Regularly

Software updates are important to your digital safety and cyber security. Think of a software patch as an armor that repels attacks and protects against various exploits. However, with the sheer number of vulnerabilities being exposed all the time many IT departments struggle to keep pace in the arms race between the hackers discovering security holes and the "good guys" releasing patches to cover them up.

Continue reading on next page >

BUSINESS DEFENSIVE CYBERSECURITY CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

⑤ Make It Easy For Employees to Escalate

Between our policies and constant communication, your staff is definitely paying attention! But paying attention isn't enough by itself if employees don't know what to do when they encounter something suspicious. By making it easy to report an issue and get help, we have dramatically increased engagement and often prevent staff from taking risky action. However, you approach this make sure to keep a record of the kinds of questions and issues that come in so that you can identify trends and create better training..

⑥ Stay Up-to-Date on Emerging Tech

Keeping up to date with technology is essential for every business owner, even those who don't run technology companies. technology helps organizations maintain a competitive edge.

- How to Keep Up-To-Date with Technology in Your Business
- 7 ways to keep up with emerging tech: CIO tips
- The Importance Of Keeping Up With Technology In The Workplace

Disaster Recovery ⑦

A set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

- What are the Best Disaster Recovery Practices for 2019?
- IT Disaster Recovery Plan

Backups and Verification ⑧

A 3-2-1 strategy means having at least 3 total copies of your data, 2 of which are local but on different mediums (viz. Tape, and Disk), and at least one copy offsite.

- 3-2-1 Backup Strategies
- Verify All Backups

Business Continuity ⑨

A plan to deal with difficult situations, so your organization can continue to function with as little disruption as possible.

It provides a way to mitigate threats, putting in place a framework which allows key functions of the business to continue even if the worst happens..

- Introduction to Business Continuity
- Business Continuity Plan

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

BUSINESS DEFENSIVE CYBERSECURITY CHEAT SHEET

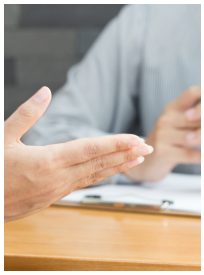
(CONTINUED)

10 Incident Response

An organized approach to addressing and managing the aftermath of a security breach or cyberattack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

- What is Incident Response?
- 6 Phases In The Incident Response Plan

11 Hiring CISO/IT/Programmers



it's tough to recruit IT talent. With more open jobs than people to fill them and the market at near full employment There simply aren't enough on the market to meet the demands of an increasingly digital workforce

- Hiring Your First CISO: A How-to
- Too few cybersecurity professionals is a gigantic problem for 2019
- It Takes an Average of 3 to 6 Months to Fill a Cybersecurity Job
- How to hire the best cybersecurity talent

12 Sandboxes

A "sandbox" is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading.

- What is Sandbox Security?
- Not All Sandboxes Are Created Equal

13 Honey Pots

A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

- What is a honeypot?
- A Honeypot Guide: Why Researchers Use Honeypots for Malware Analysis
- Building a Basic Honeypot

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH