BUILDing for Growth Workshop

IT Systems and Cybersecurity in the Age of Trolls, Phishing, Malware, and Ransomware

Dan Hernandez
Owner and Founder
Professional Computer Support

April 28th
10:30-11:30am Pacific
BUILDing for Growth
Selected Cohort
## Overall Identified Challenges

<table>
<thead>
<tr>
<th>STAFF</th>
<th>SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Naming and prioritizing needs</td>
<td>▪ Human Resources</td>
</tr>
<tr>
<td>▪ Communication</td>
<td>▪ Organizational Structure &amp; Mid-Level Management</td>
</tr>
<tr>
<td>▪ Organizational Culture</td>
<td>▪ Facilities &amp; COVID response</td>
</tr>
<tr>
<td>▪ Skills &amp; Development</td>
<td>▪ Operations &amp; Systems</td>
</tr>
<tr>
<td>▪ Executive Leadership &amp; Decision-Making</td>
<td>▪ <strong>Information Technology</strong></td>
</tr>
<tr>
<td>▪ Leadership Transitions</td>
<td>▪ Fund Development, Management &amp; Long-Term Financial Stability</td>
</tr>
</tbody>
</table>
Getting the Most from Today’s Workshop

**Introduce Yourself**
Post the organization you’re representing, your role, & location in chat

**Ask Questions**
Use the “Raise Hand” function or post questions in chat

**Share Your Experience**
Offer your own perspective & experience to your peers

We will cover a lot at a high level, but we will our best to address specific questions.
Workshop Learning Goals

By the end of this workshop, you will have:

- A clear understanding of how to manage your IT with rapid growth while protecting your business from cyber crime, ransomware and phishing emails.
Today We’re Going To Cover

• The key IT items to implement to protect your business.
• The #1 security threat to your business that antivirus, firewalls and other security protocols can’t protect against.
• Why firewalls and antivirus software aren’t enough anymore.
We’re Going To Cover...

How To Avoid Being A Sitting Duck To Cybercriminals And Protect Everything You’ve Worked So Hard To Achieve
Why The Heck Do You Care What I Have To Say?
My Story
The Biggest Danger Is Your Complacency

“Success breeds complacency. Complacency breeds failure. Only the paranoid survive.”

- Andrew Grove, former CEO of Intel
Our Community is Under Attack
Thousands Of Small Businesses Are Being Ransomed, Phished And Scammed Out Of Hundreds Of Thousands Of Dollars Which You Never See In The News
Mid-Size Non-Profit
SF Bay Area
Phished CFO for email credentials

Monitored emails and waited for opportunity

Created a fake domain name with one character off

Re-directed 137k wire transfer
All Businesses Are At Risk

- Small Business
- Big Business
- Business in the cloud
- All Business
Hackers Stole $650,000 From Nonprofit and Got Away, Showing Limits to Law Enforcement's Reach

When criminals swindled One Treasure Island, the San Francisco organization turned to the cops. Getting no help, its director decided to launch her own investigation
A Quick Overview Of The Sophistication And Proliferation Of The Cybercrime Business
80 Million Households And 7 Million Small To Medium Businesses HACKED
The Digital Underground's Thriving Black Market

- Credit card details: $2 to $90
- Physical credit cards: $190
- Card cloners: $200-$300
- Setting up email accounts with 1 character off can easily be created impersonating users
- Anyone can easily buy training, tools and services for committing fraud, hacking systems, buying stolen credit cards, setting up fake websites, etc.
82,000 NEW Malware Threats Are Being Released Per Day

Source: PC World
Ransom attacks are when a hacker gains access to your network and encrypts all your data.

That’s sort of what’s happening in the cybercrime world — sensitive data in the wrong hands is used to extort money.
Secure Remote Work

• Hybrid work is now a reality for many businesses

• 70% of businesses plan to adopt hybrid work - Mercer study

• 58% of employees want full-time remote work post-pandemic and 39% want some hybrid - FlexJobs survey

• Over half of men (52%) and women (60%) say they would quit without remote options - FlexJobs

• 81% of IT pros believed that remote work increases enterprise cybersecurity challenges - 2021 Digital Readiness Survey
Zero Trust & MFA

What is Zero Trust?
• Starts with strongly validated identity
  • Requires multi-factor authentication (MFA)
• Users **only** allowed access based on role needs
  • Least privilege principle applied everywhere
  • Zero Trust applied internally as much as externally

Identity validation paramount to Zero Trust
• Passwords alone insufficient
• Passwordless models not always true MFA
• MFA a requirement
• Continuous, contextual adaptive risk assessment helps
Over 90% of cyberattacks and malware infections start with malicious email - Trend Micro and many others

- FBI IC3 reports 7.8 times more BEC crime reports than ransomware reports.
  - BEC accounts for 1.8B in losses, ransomware $29
  - Accounts for 37% of cyberattack loses 2020

- Phishing increases over other mediums
  - SMSishing (text phishing)
  - Messager apps
    - WhatsApp
    - FB Messenger
    - Slack
    - Discord
    - Etc.
Social Media

Threat #1: Security

600,000 Facebook Accounts Are Hacked Every Single DAY.
Bank Fraud:

FDIC Does NOT Protect You From Bank Fraud; And The Bank Is NOT Responsible For Getting Your Money Back!!!
The Next Frontier: MOBILE

Mobile malware growth accelerating
Mobile Computing **Dangers On The Rise...**

If A Device Is **Lost Or Stolen**, And The Data Was NOT Encrypted, You May Have Violated A California Data Breach Law

- Small list of organizations having to report to the State data breaches.
- Anthem Blue Cross
- The San Francisco Symphony
- California Pizza Kitchen
- Sonoma Valley Healthcare Districts
“Spam remains the single biggest driver of big breaches today. If we look at some of the biggest data breaches in recent memory - JPMorgan, Target, RSA Security come to mind - they all began with poisoned e-mail.”

– Brian Krebs, Spam Nation
Cyber Insurance Evolution and Rising Costs

Paying ransom has lost insurers profit

They will turn those costs and security compliance mandates on you
Why do we need Ransomware Cyber Insurance
Insurance Companies Hate Paying Ransoms
Accessing networks and denying claims
**Self-Assessment Questionnaire**

**NETWORK SECURITY CONTROLS**

7. Indicate whether the Applicant currently has the following in place:

   a. A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices
   b. Up-to-date, active firewall technology
   c. Up-to-date, active anti-virus software on all computers, networks, and mobile devices
   d. A process in place to regularly download, test, and install patches
      - If Yes, is this process automated?
      - If Yes, are critical patches installed within 30 days of release?
   e. Intrusion Detection System (IDS)
   f. Intrusion Prevention System (IPS)
   g. Data Loss Prevention System (DLP)
   h. Multi-factor authentication for administrative or privileged access
   i. Multi-factor authentication for remote access to the Applicant’s network and other systems and programs that contain private or sensitive data in bulk
   j. Multi-factor authentication for remote access to email
   k. Remote access to the Applicant’s network limited to VPN
   l. Backup and recovery procedures in place for all important business and customer data
      - If Yes, are such procedures automated?
      - If Yes, are such procedures tested on an annual basis?
   m. Annual penetration testing
   n. Annual network security assessments
   o. Systematic storage and monitoring of network and security logs
   p. Enforced password complexity requirements
   q. Procedures in place to terminate user access rights as part of the employee exit process

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>j</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>k</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>l</td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>m</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>q</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The 5-Question Test:

• Do you have **MFA** for email and sensitive information?
• Do you have **backups** and are you sure they are working?
• Do you have **up-to-date, active antivirus** installed on all computers?
• Do you have a written documented **breach response plan**?
• Do you have **up-to-date, active firewall** technology?
So How Do You Protect Yourself?
Must Have IT Components

- Security awareness training; You are only as strong as your weakest employee.

- Strong passwords in use. Not reusing passwords or sharing in a spreadsheet. You must have a password manager.

- No personal devices except cell phones. If you use a cell phone you must have a password key on the device and a multi factor authentication turned on.
Tips For Protecting Yourself:

• Cancel your debit cards; they are the #1 way bank accounts get compromised.
• Have a dedicated PC for online banking and DON'T use that PC for accessing any other websites, e-mail access, social media sites or for downloading applications.
• Sign up for e-mail alerts from your bank whenever a withdrawal over $100 happens.
• Require YOUR signature for any wire transfers.
• Have your money spread out in multiple accounts to minimize the risk.
IT Management

• IT written security policy added to employment manual.
• Following written onboarding process between your HR department and your IT department.
• Device Management and tracking
• Backup all data to the cloud
• Turn on Multi factor authentication whenever possible
• Use a password manager
• Firewall must be up to date, patched and managed.
• Spam filter.
• Force passwords that are difficult to hack (Password Manager).
• Back up your systems properly (protects against a number of threats).
• Employee education Security Awareness Training (SAT).
• Lock down the ability for employees to use home PCs and devices to access your network and cloud applications.
• Documented onboarding process.
Bottom Line:

You Need To Get Serious About Protecting Your Company Against Cybercrime!

But What Does That Look Like?
3 Steps To Protecting Your Organization:

• **Step 1: Threat Assessment (3rd party Assessment)**
  A third party assessment is performed by an assessment organization independent of the customer-supplier relationship and is free of any conflict of interest.

• **Step 2: Action Plan**
  Based on what’s discovered, what do we need to do to ensure our systems, data and operations are secure from theft, compromise, corruption, etc.?

• **Step 3: Ongoing Maintenance**
  You don’t want to take a “set-it-and-forget-it” approach to security – your attackers won’t!
At no cost or obligation, we’ll conduct a “Threat Assessment” where we’ll:

- Provide Cyber Security Assessment
- Review on premise devices
- Review Firewalls, antivirus applications
- Review cell phone policies, backups, employee training, etc.
SECURITY PLUS 2022

- SECURITY PLUS
  SAME AS ABOVE

$57 PER USER

SAAS BACKUP OFFICE 365
MANAGED ADVANCED ENDPOINT DEFENSE

ZERO TRUST
BY THREATLOCKER
SECURE EMAIL & COLLABORATION
SPAM/PHISHING FILTER

WE ESTABLISH TRUST BY VALUING RELATIONSHIPS AND GOING BEYOND JUST SERVICE.
WE DELIVER ADDED VALUE INCLUDING EDUCATION, ADVISING, COLLABORATING & STRATEGIZING.

SECURITY PLUS
SAME AS ABOVE
We Go Further

Why PCS Is Your Best Choice For Business Technology Solutions.

We partner with you to provide worry free growth of your business.
We offer software & infrastructure solutions.
We establish trust by valuing relationship and going beyond just service.
We deliver added value including education, advising, collaborating & strategizing.
Exit Poll
Thank you!

Dan Hernandez
Dan@pcs-sf.com