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

La Piana CONSULTING

FORDFOUNDATION

BUILDing for Growth

Selected Cohort

AlternateROOTS
ARTS • COMMUNITY • ACTIVISM

ALLIED MEDIA PROJECTS

STATEVOICES

ASHÉ CULTURAL ARTS CENTER

Black in AI

NATIONAL DOMESTIC WORKERS ALLIANCE

Borealis PHILANTHROPY

MOVEMENT ALLIANCE PROJECT

DISABILITY RIGHTS FUND

NBWC
NATIONAL BLACK WORKER CENTER

Justice for Migrant Women

NATIONAL WOMEN'S LAW CENTER

Rockwood Leadership Institute

JOBS WITH JUSTICE

BLACK YOUTH PROJECT 100
BYP 100
UNAPOLOGETICALLY BLACK

THE LOHM

CENTRAL FLORIDA JOBS WITH JUSTICE

FIRELIGHT
CHANGING THE STORY

BLACK VOTERS MATTER

THE CENTER FOR POPULAR DEMOCRACY

REPAIRERS OF THE BREACH

NELP NATIONAL EMPLOYMENT LAW PROJECT

RUTGERS
School of Management and Labor Relations
Center for Innovation in Worker Organization

STUDIO MUSEUM HARLEM

ROOSEVELT INSTITUTE
REIMAGINE THE RULES

THE FOUR FREEDOMS FUND
A fund of NEO Philanthropy

OCF

Transgender Law Center

First Peoples Fund

Overall Identified Challenges

STAFF	SYSTEMS
▪ Naming and prioritizing needs ▪ Communication ▪ Organizational Culture ▪ Skills & Development ▪ Executive Leadership & Decision-Making ▪ Leadership Transitions	▪ Human Resources ▪ Organizational Structure & Mid-Level Management ▪ Facilities & COVID response ▪ Operations & Systems ▪ **Information Technology** ▪ Fund Development, Management & Long-Term Financial Stability

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.

ProfessionalComputer
SUPPORT

We're Going To Cover…

How To Avoid Being A **Sitting Duck** To Cybercriminals And Protect Everything You've *Worked So Hard To Achieve*

ProfessionalComputer
SUPPORT

Why The Heck Do You Care What I Have To Say?

ProfessionalComputer
SUPPORT

My Story

ProfessionalComputer
SUPPORT

The Biggest Danger Is Your Complacency

"Success breeds complacency. Complacency breeds failure. Only the paranoid survive."

- Andrew Grove, former CEO of Intel

ProfessionalComputer
SUPPORT

Our Community is Under Attack

ProfessionalComputer
SUPPORT

Thousands Of Small Businesses Are Being Ransomed, Phished And Scammed Out Of Hundreds Of Thousands Of Dollars Which You Never See In The News

ProfessionalComputer
SUPPORT

Mid-Size Non-Profit

SF Bay Area

Mid-Size Non-Profit

Phishing Scam

- 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

ProfessionalComputer
SUPPORT

All Businesses Are At Risk

Small Business

Big Business

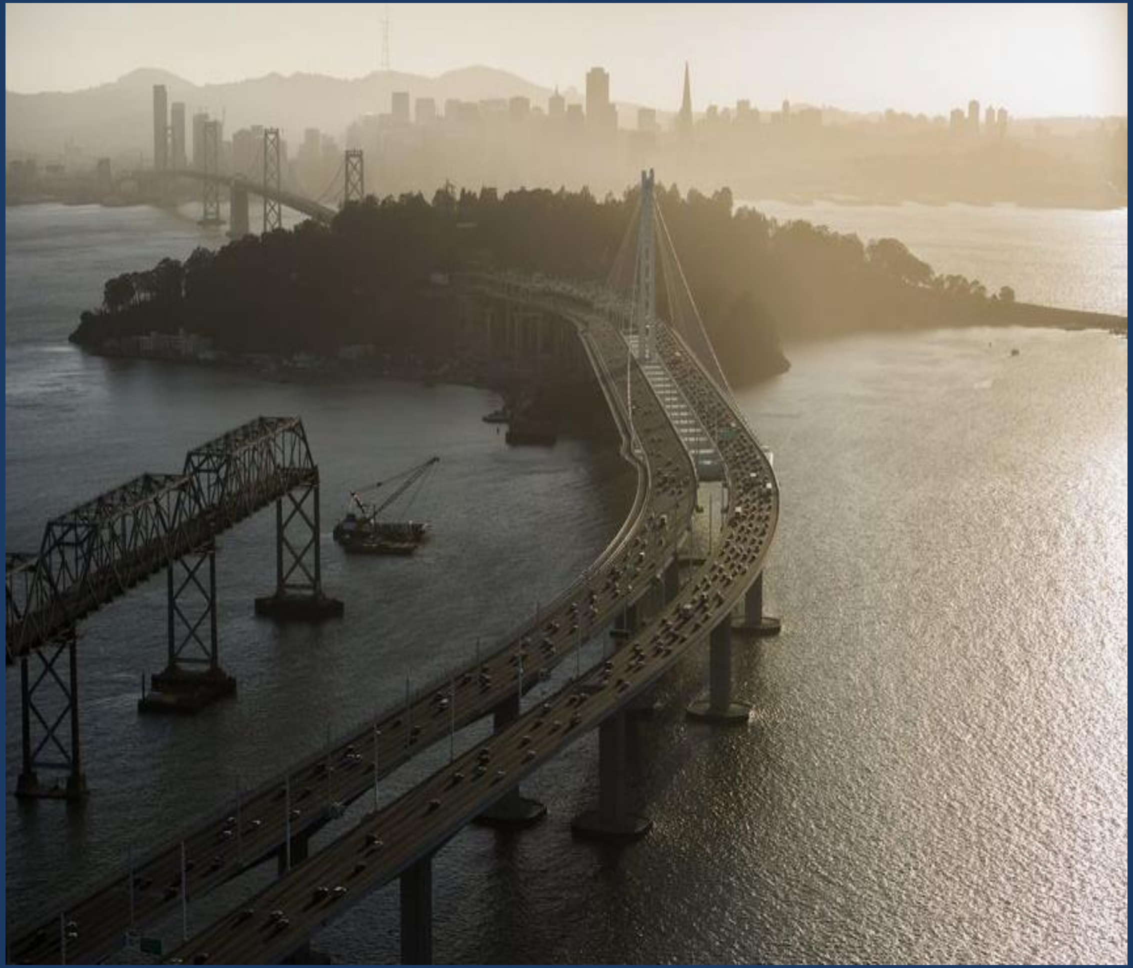
Business in the cloud

All Business

ProfessionalComputer
SUPPORT

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



ProfessionalComputer
SUPPORT

A Quick Overview Of The Sophistication And Proliferation Of The Cybercrime Business

ProfessionalComputer
SUPPORT

80 Million Households And 7 Million Small To Medium Businesses HACKED

ProfessionalComputer
SUPPORT

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.

ProfessionalComputer
SUPPORT

82,000

NEW Malware Threats Are Being Released *Per Day*

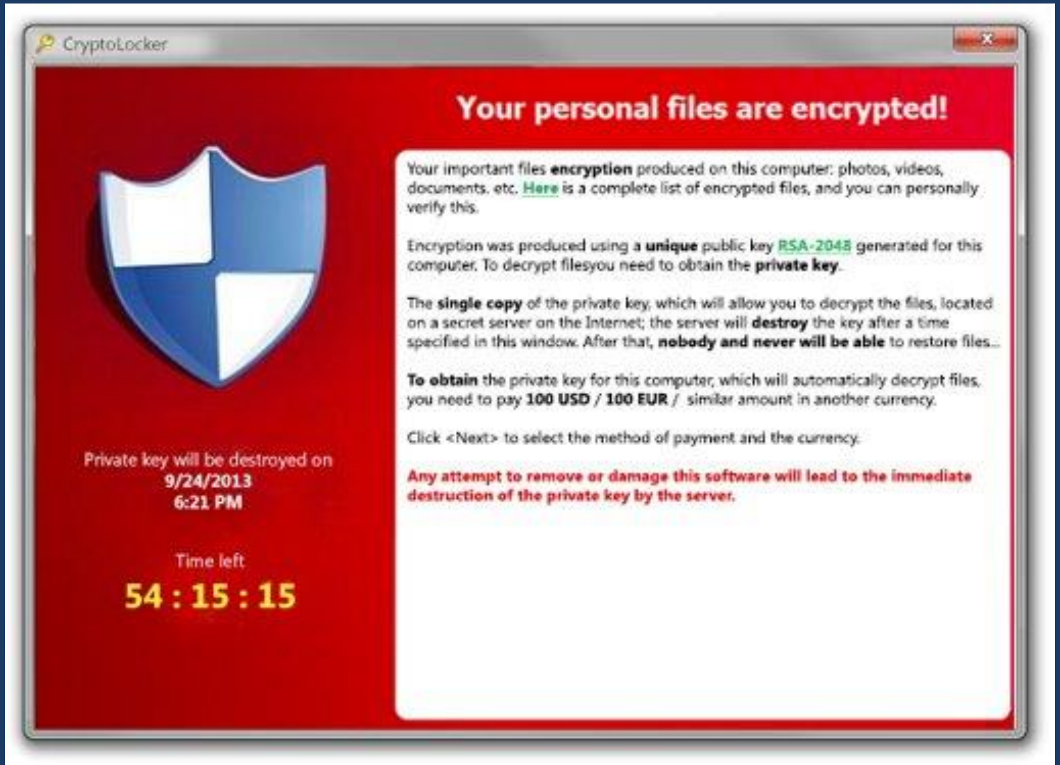
Source: PC World

ProfessionalComputer
SUPPORT

Ransomware Dangers On The Rise…

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.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

ProfessionalComputer
SUPPORT

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% wat 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*

ProfessionalComputer
SUPPORT

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

ProfessionalComputer
SUPPORT

Business Email Compromise (BEC) & Spear Phishing

Over 90% of cyberattacks and malware infections start with malicious email - *Trend Micro and many others*

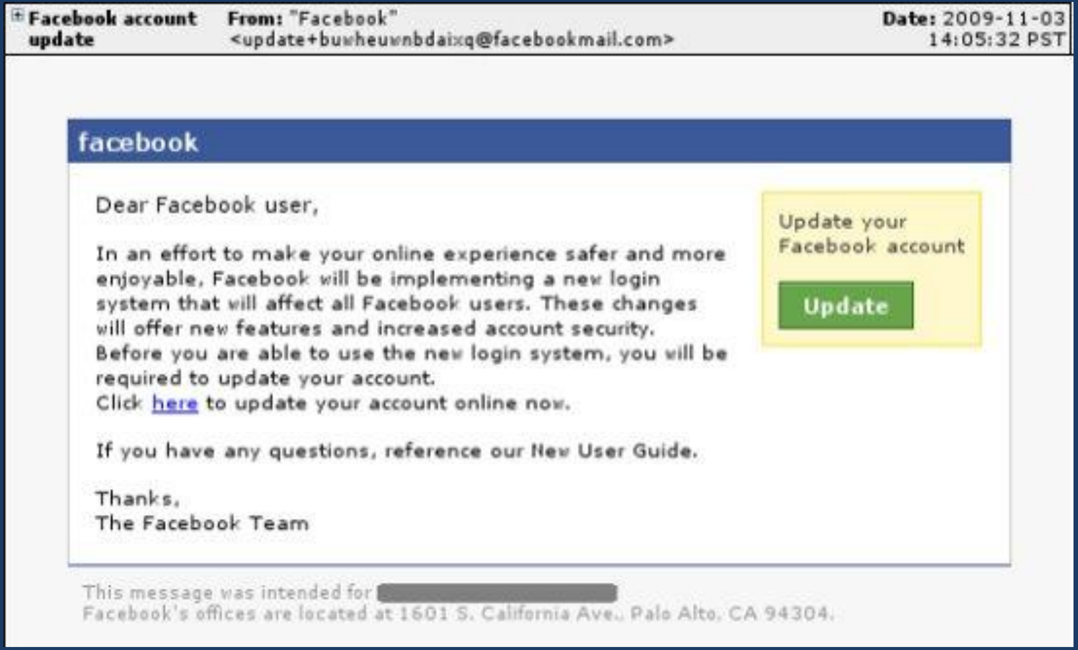
- FBI IC3 reports 7.8 times more BEC crime reports than ransomware reports.
  - BEC accounts for 1.8B in losses, ransomware $29
  - Accounts for 37% of cyberattack loses 2020

- Phishing increases over other mediums
  - SMSishing (text phishing)
  - Messager apps
    - WhatsAPP
    - FB Messanger
    - Slack
    - Discord
    - Etc.

Social Media

Threat #1: Security

600,000 Facebook Accounts Are Hacked <u>Every Single DAY</u>.



Facebook account update **From:** "Facebook" <update+buwheuwnbdaixq@facebookmail.com> **Date:** 2009-11-03 14:05:32 PST

facebook

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account.
Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

Update your Facebook account

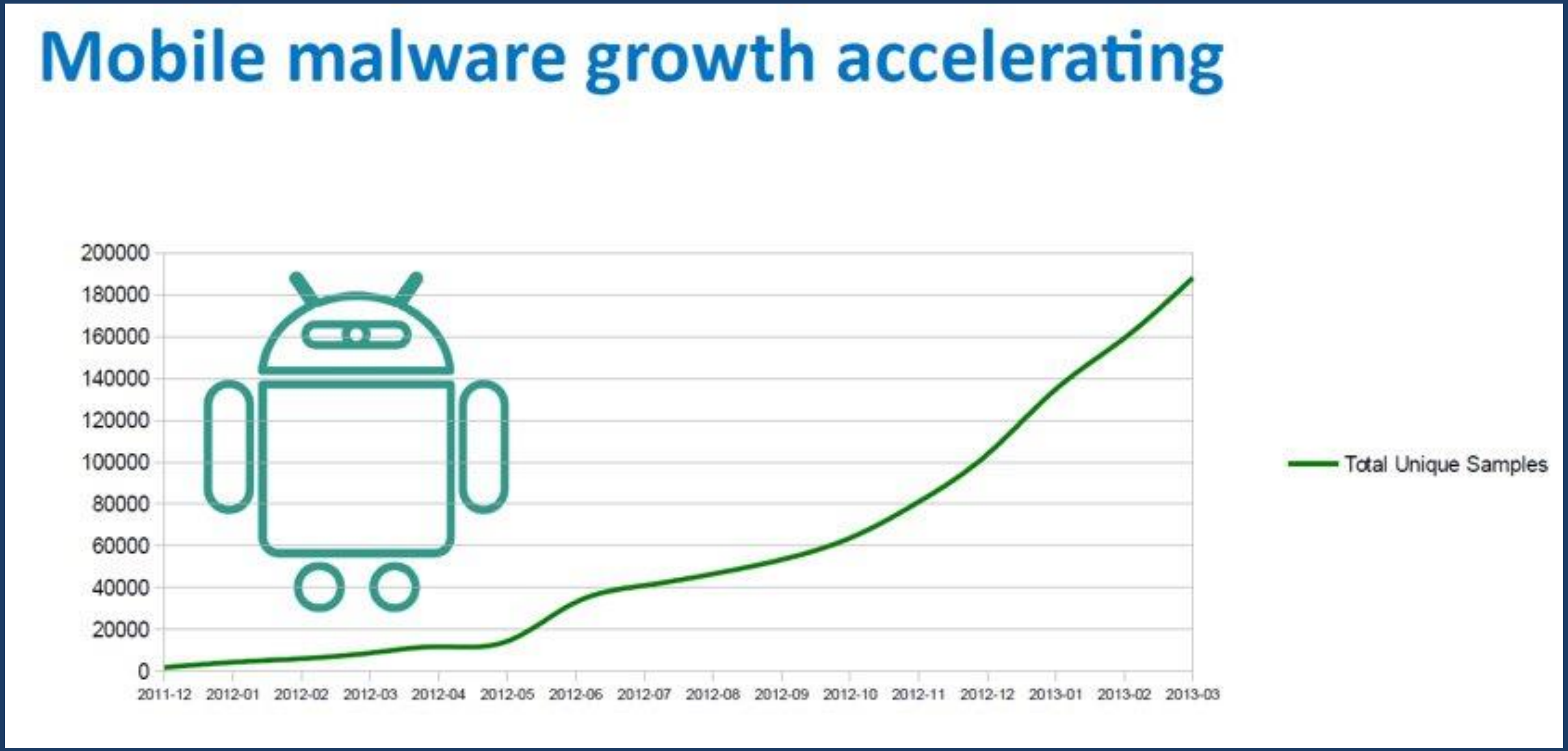
Update

This message was intended for [redacted]
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

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



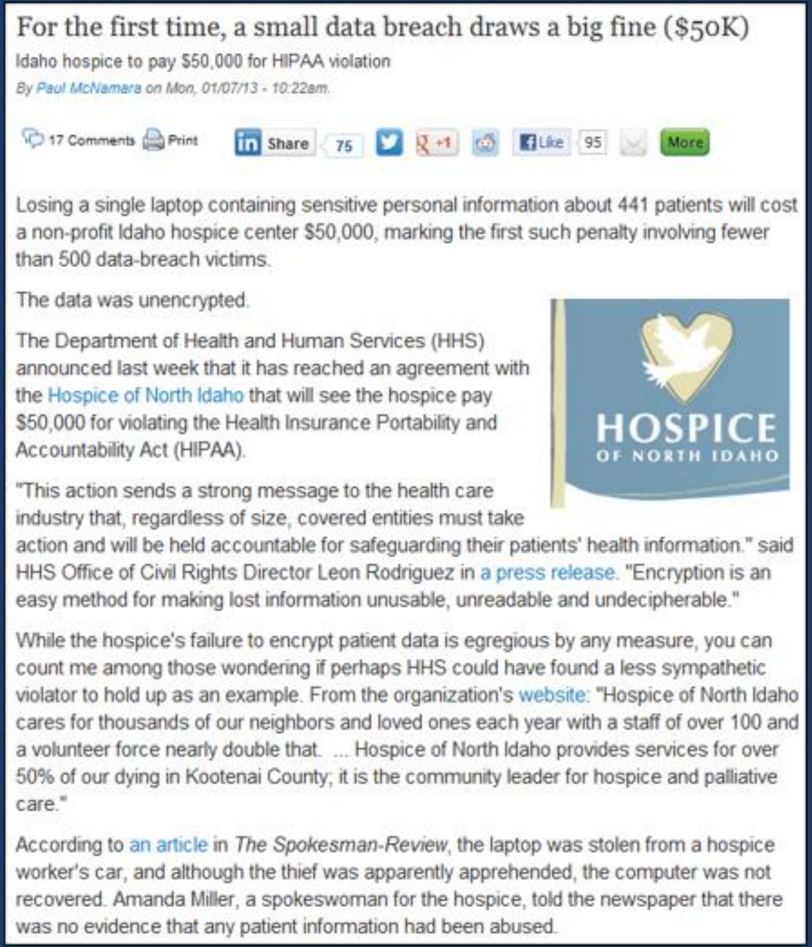
Mobile malware growth accelerating

ProfessionalComputer
SUPPORT

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



For the first time, a small data breach draws a big fine ($50K)

Idaho hospice to pay $50,000 for HIPAA violation

By Paul McNamara on Mon, 01/07/13 - 10:22am.

Losing a single laptop containing sensitive personal information about 441 patients will cost a non-profit Idaho hospice center $50,000, marking the first such penalty involving fewer than 500 data-breach victims.

The data was unencrypted.

The Department of Health and Human Services (HHS) announced last week that it has reached an agreement with the Hospice of North Idaho that will see the hospice pay $50,000 for violating the Health Insurance Portability and Accountability Act (HIPAA).

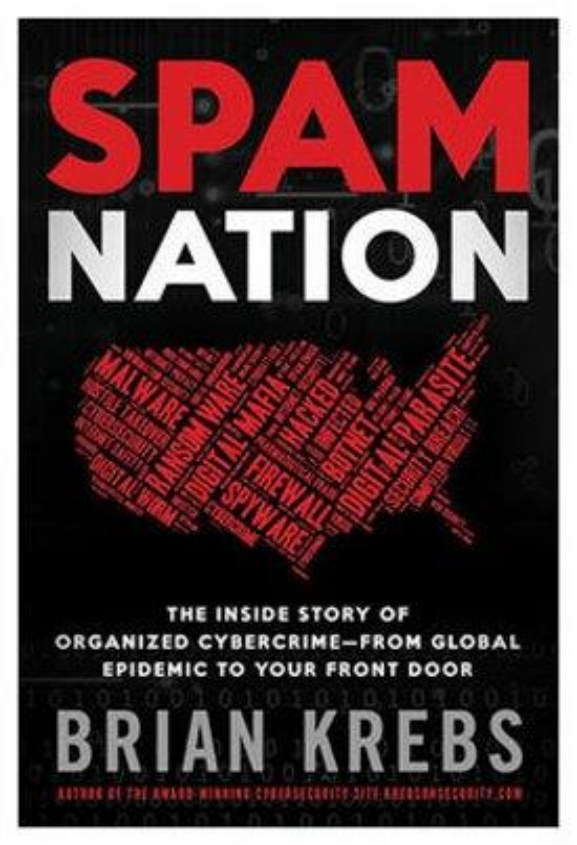
"This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information," said HHS Office of Civil Rights Director Leon Rodriguez in a press release. "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."

While the hospice's failure to encrypt patient data is egregious by any measure, you can count me among those wondering if perhaps HHS could have found a less sympathetic violator to hold up as an example. From the organization's website: "Hospice of North Idaho cares for thousands of our neighbors and loved ones each year with a staff of over 100 and a volunteer force nearly double that. ... Hospice of North Idaho provides services for over 50% of our dying in Kootenai County; it is the community leader for hospice and palliative care."

According to an article in *The Spokesman-Review*, the laptop was stolen from a hospice worker's car, and although the thief was apparently apprehended, the computer was not recovered. Amanda Miller, a spokeswoman for the hospice, told the newspaper that there was no evidence that any patient information had been abused.

ProfessionalComputer
SUPPORT

Spam!


SPAM NATION
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
AUTHOR OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

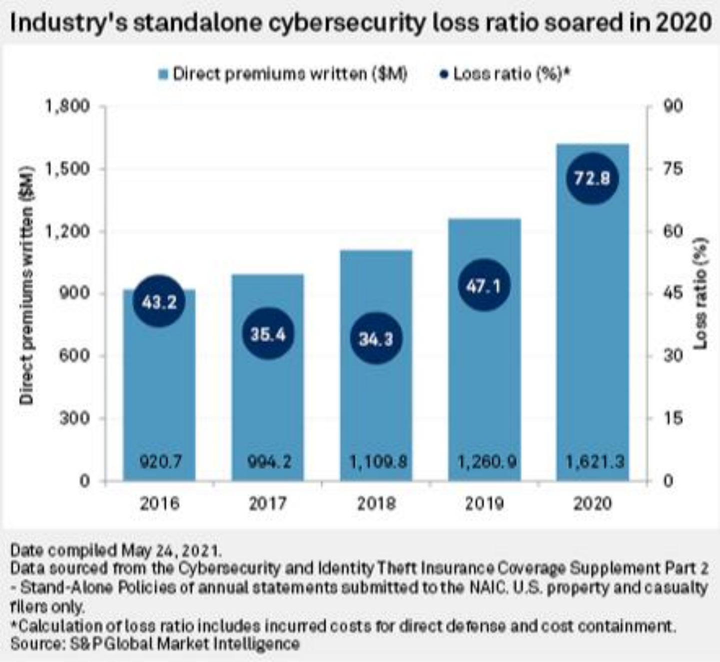
"Spam remains the single biggest driver of big breaches today. If we look at some of the biggest data breaches in recent memory - JPMorgan, Target, RSA Security come to mind - they all began with poisoned e-mail."

– Brian Krebs, Spam Nation

ProfessionalComputer
SUPPORT

Cyber Insurance Evolution and Rising Costs

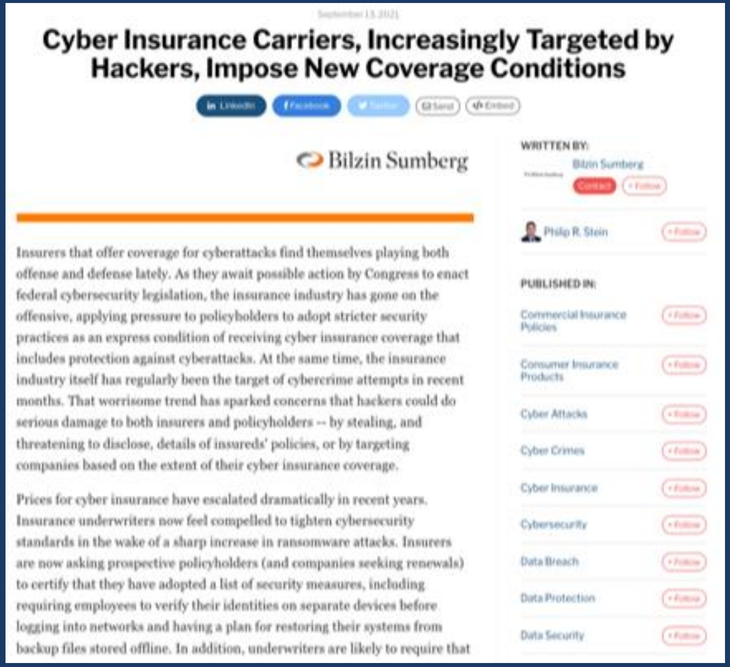
Paying ransom has lost insurers profit



Industry's standalone cybersecurity loss ratio soared in 2020

Date compiled May 24, 2021.
Data sourced from the Cybersecurity and Identity Theft Insurance Coverage Supplement Part 2 - Stand-Alone Policies of annual statements submitted to the NAIC. U.S. property and casualty filers only.
*Calculation of loss ratio includes incurred costs for direct defense and cost containment.
Source: S&P Global Market Intelligence

They will turn those costs and
security compliance mandates on you



September 13, 2021

Cyber Insurance Carriers, Increasingly Targeted by Hackers, Impose New Coverage Conditions

Insurers that offer coverage for cyberattacks find themselves playing both offense and defense lately. As they await possible action by Congress to enact federal cybersecurity legislation, the insurance industry has gone on the offensive, applying pressure to policyholders to adopt stricter security practices as an express condition of receiving cyber insurance coverage that includes protection against cyberattacks. At the same time, the insurance industry itself has regularly been the target of cybercrime attempts in recent months. That worrisome trend has sparked concerns that hackers could do serious damage to both insurers and policyholders -- by stealing, and threatening to disclose, details of insureds' policies, or by targeting companies based on the extent of their cyber insurance coverage.

Prices for cyber insurance have escalated dramatically in recent years. Insurance underwriters now feel compelled to tighten cybersecurity standards in the wake of a sharp increase in ransomware attacks. Insurers are now asking prospective policyholders (and companies seeking renewals) to certify that they have adopted a list of security measures, including requiring employees to verify their identities on separate devices before logging into networks and having a plan for restoring their systems from backup files stored offline. In addition, underwriters are likely to require that

WRITTEN BY:

Bilzin Sumberg

Contact + Follow

Philip R. Stein + Follow

PUBLISHED IN:

Commercial Insurance Policies + Follow

Consumer Insurance Products + Follow

Cyber Attacks + Follow

Cyber Crimes + Follow

Cyber Insurance + Follow

Cybersecurity + Follow

Data Breach + Follow

Data Protection + Follow

Data Security + Follow

ProfessionalComputer
SUPPORT

Why do we need Ransomware

Cyber Insurance

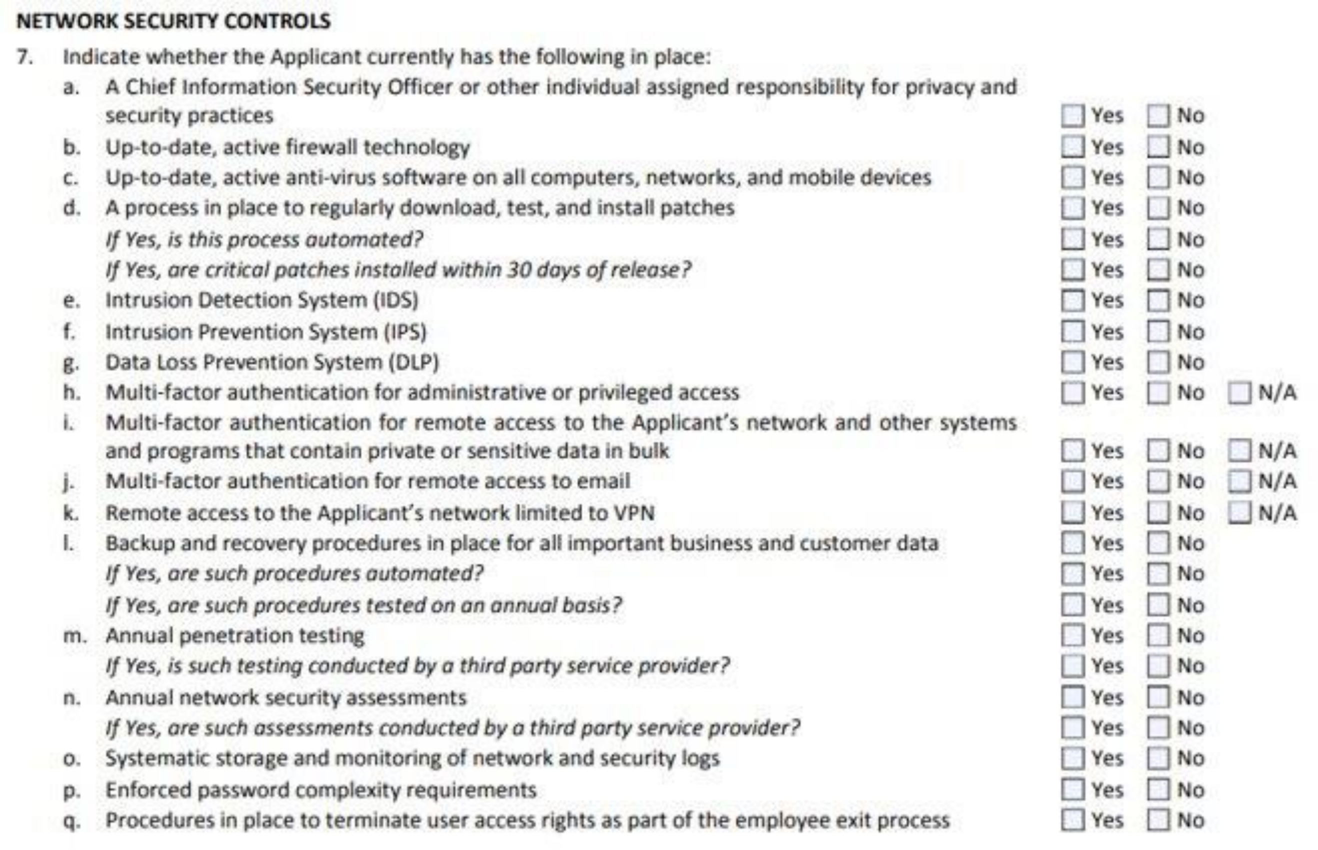
ProfessionalComputer
SUPPORT

Insurance Companies Hate Paying Ransoms

Accessing networks and **denying claims**

ProfessionalComputer
SUPPORT

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	□ Yes	□ No	
b.	Up-to-date, active firewall technology	□ Yes	□ No	
c.	Up-to-date, active anti-virus software on all computers, networks, and mobile devices	□ Yes	□ No	
d.	A process in place to regularly download, test, and install patches	□ Yes	□ No	
	If Yes, is this process automated?	□ Yes	□ No	
	If Yes, are critical patches installed within 30 days of release?	□ Yes	□ No	
e.	Intrusion Detection System (IDS)	□ Yes	□ No	
f.	Intrusion Prevention System (IPS)	□ Yes	□ No	
g.	Data Loss Prevention System (DLP)	□ Yes	□ No	
h.	Multi-factor authentication for administrative or privileged access	□ Yes	□ No	□ N/A
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	□ Yes	□ No	□ N/A
j.	Multi-factor authentication for remote access to email	□ Yes	□ No	□ N/A
k.	Remote access to the Applicant's network limited to VPN	□ Yes	□ No	□ N/A
l.	Backup and recovery procedures in place for all important business and customer data	□ Yes	□ No	
	If Yes, are such procedures automated?	□ Yes	□ No	
	If Yes, are such procedures tested on an annual basis?	□ Yes	□ No	
m.	Annual penetration testing	□ Yes	□ No	
	If Yes, is such testing conducted by a third party service provider?	□ Yes	□ No	
n.	Annual network security assessments	□ Yes	□ No	
	If Yes, are such assessments conducted by a third party service provider?	□ Yes	□ No	
o.	Systematic storage and monitoring of network and security logs	□ Yes	□ No	
p.	Enforced password complexity requirements	□ Yes	□ No	
q.	Procedures in place to terminate user access rights as part of the employee exit process	□ Yes	□ No	

ProfessionalComputer
SUPPORT

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?

ProfessionalComputer
SUPPORT

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.

ProfessionalComputer
SUPPORT

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.

ProfessionalComputer
SUPPORT

Bottom Line:

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

But What Does That Look Like?

ProfessionalComputer
SUPPORT

3 Steps To Protecting Your Organization:

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

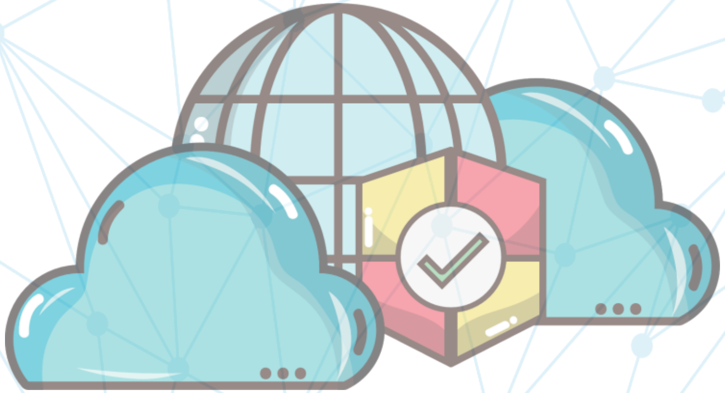
- **Step 2: Action Plan**
  Based on what's discovered, what do we need to do to ensure our systems, data and operations are secure from theft, compromise, corruption, etc.?

- **Step 3: Ongoing Maintenance**
  You don't want to take a "set-it-and-forget-it" approach to security – your attackers won't!

The First Step Is Free

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

$35 PER USER

BLOKWORX

MAED
Managed Advanced Endpoint Defense

PIIGuard360

Cyber Guard 360
Security Awareness Training

Dark Web Monitoring

PCS PROFESSIONAL COMPUTER SUPPORT

IT'S WHO WE ARE. IT'S HOW WE WORK. IT'S HOW WE ADVOCATE FOR OURSELVES, EACH OTHER, OUR TEAM AND OUR CLIENTS.

SECURITY PLUS 2022

$57 PER USER

- SECURITY PLUS
  SAME AS ABOVE

SAAS BACKUP OFFICE 365

MANAGED ADVANCED
ENDPOINT DEFENSE

ZERO TRUST

BY THREATLOCKER

SECURE EMAIL & COLLABORATION

SPAM/PHISING FILTER

THREATLOCKER

PCS PROFESSIONAL COMPUTER SUPPORT

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

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.

ProfessionalComputer
SUPPORT

Exit Poll

Thank you!

Dan Hernandez
Dan@pcs-sf.com

La Piana
CONSULTING