

# Why CyberSecurity is HR's Business

What You Must Know To Protect Your HR & Other Business Assets



Daniel Foote  
CEO

Mary M. Rydesky  
EVP



DanTech Services, Inc.



## A True Story



## Today We're Going To Cover

- How an Acceptable Use Policy (AUP) can protect your business
- Gaining End User Compliance
- Security takes a team culture
- Mobile Device Management & the consequences of neglect
- Why HR must lead in data protection



## Ultimately We Will Address...

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



## Who is Dan Foote?

- Dan Foote is the CEO of DanTech Services in Anchorage, Alaska & author of *Under Attack*, a #1 best seller
- Started DanTech Services in 2005 to provide personalized services & support for Alaska businesses
- DanTech Services provides a layered approach to data & network security
- Works to keep Computers Under Control!™



## Who is Mary Rydesky?

- Mary has one foot in the HR world, the other in IT
- Worked for large corporations & hospitals to integrate policies & practices that focus on getting the job done
- Endorses an HR/IT coalition to train for a safe computer culture
- Holds Masters in Information Science & Business Administration (MBA)
- Pursuing her doctorate in Human Resources & Technology
- As a trainer & consultant, she works with DanTech Services to keep "Computers under Control!™"



## Questions



## SHRM Headlines of 2017

- [New Mexico Enacts Data Breach Notification Act](#) (4/26/17)
- [HR Beware: 'Tis the Season for W-2 Scams](#) (4/11/2017)
- [Boeing Insider Data Breach Serves as Reminder for HR](#) (3/10/17)



## The Biggest Danger Is Your Complacency

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

- Andrew Grove, former CEO of Intel



## What & Why

- Threats are External
  - And internal
- Relying only on IT leads to...
  - Complacency
  - Neglect
- Personnel decisions are key
  - Hiring
  - Training



## A Quick Overview Of The Sophistication & Proliferation Of The Cybercrime Business



## What Do You Need to Protect?

- Compensation, payroll, tax
- Personal information (identity theft)
- HIPAA information
- Training / certification records
- Contracts
- Correspondence
- Performance analytics



## Data Breach

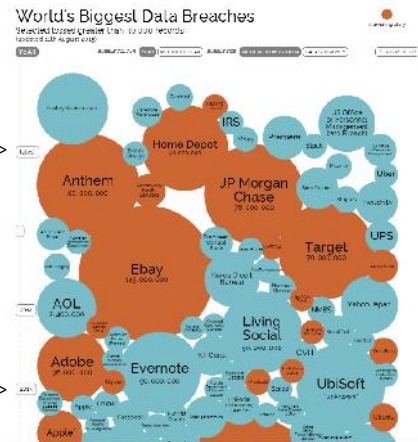
- A **data breach** is an incident in which sensitive, protected or confidential **data** has potentially been viewed, stolen or used by an individual unauthorized to do so
- **Data breaches** may involve personal health information (PHI), personally identifiable information (PII), trade secrets / intellectual property



## Polymorphic Malware

1 Million NEW Malware Threats Are Being Released Per Day

## The Evolution Of Internet Crime



Snapshot as of 9/2015

Graphic: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



2016>

2015>

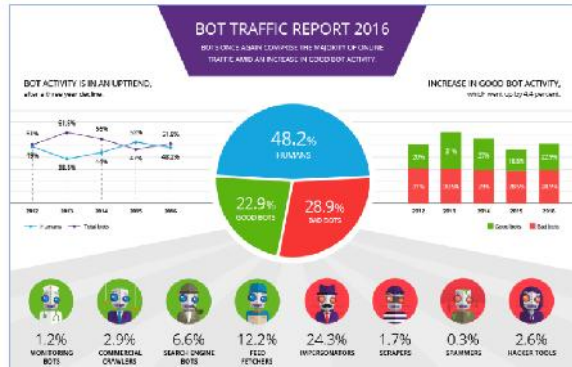
2010>

## ...the explosion in 2 years...

Snapshot as of 3/2017

Graphic: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

## Botnet Traffic



<https://www.incapsula.com/blog/bot-traffic-report-2016.html>

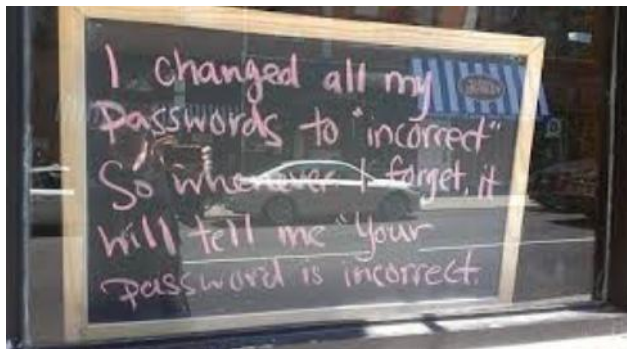


## Weak ID, Credential, & Access Mgmt.

- Data breaches & enabling of attacks can occur because of a lack of scalable identity & access management systems, failure to use multi-factor authentication, weak password use, & more



## W3@k Pa55w0rd5



## Social Engineering


- Managing social change
- (in the context of information security)

*"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."*




## Account Hijacking

- Methods include
  - phishing
  - fraud
  - exploitation of software vulnerabilities
- Attackers can
  - eavesdrop on activities & transactions
  - then manipulate data
  - return falsified info
  - redirect to illegitimate sites



## Phishing & Spear Phishing

<p>phish-ing 'fiSHiNG/ noun</p> <p>the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords &amp; credit card numbers.</p>	<p>spear phish-ing noun</p> <p>the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.</p> <p>"spear phishing represents a serious threat for every industry"</p>
--	---

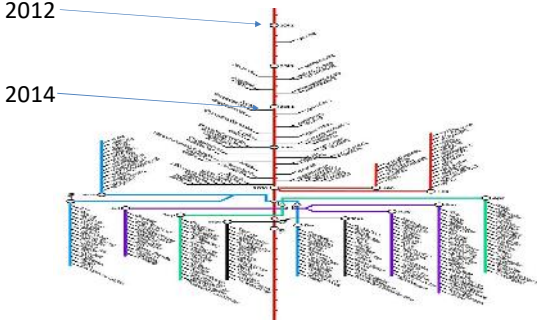


## The Digital Underground's Thriving Black Market


- Dark Web where 90% of the Internet exists
- Malware & hacking kits sold
- BitCoin (BC) is currency of choice
- Stolen data sold (credit cards, hospital records, financial records)
- Virtually untraceable

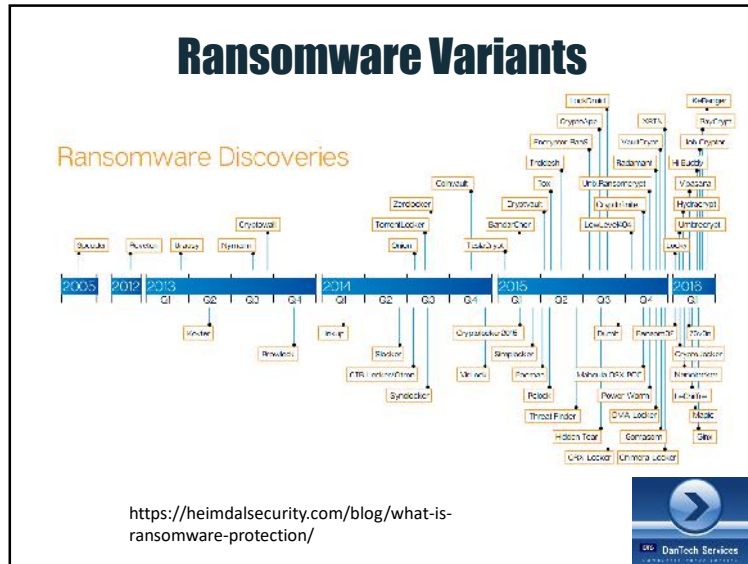



## Ransomware Explosion



<https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017>





## Ransomware is Epidemic!

HealthcareIT News

Privacy & Security UPDATE

Emerging Threats: Cybersecurity Terms

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

That's happening in the cybercrime world — sensitive data in the wrong hands is used to extort money

## Malvertising attacks unseen by most firewalls

Over 10 million Web surfers possibly exposed to malvertising

“...redirection code planted in the malicious advertisements uses SSL/TLS (Secure Sockets Layer/Transport Layer, ...”

By Jeremy Kirk, IDG News Service, Jul 27, 2015



## Valuable Data



IoT devices may be capturing your data!

- Compensation, payroll, tax
- Identity
- Entry cards & badges
- Contracts
- HIPAA
- Training records
- Company confidential
- Resumes/recruitment



## Data Loss

- Data is completely or partially lost due to
  - malicious attacks
  - corruption
  - accidental or intentional deletion
  - physical catastrophe such as a fire, earthquake or other calamity



## Malicious Insiders

- A current or former employee
  - contractor
  - other business partner
- who has or had authorized access to an
  - organization's network,
  - system
  - data
- intentionally exceeds or misuses that access



## No Is Not An Answer (Policies & Rules are Not Enough)

- Employees circumvent restrictions
- New tools (phones, tablets, cameras) make your data easy to copy
- IT 'rules' frustrate employees & sometimes interfere with legitimate work
- Lack of time results in accidentally falling for hoaxes







## The Number One Security Threat

- Can someone tell me what the **#1 Security Threat** to your business might be?

[Experts: Employees Commit Most Data Breaches](#) (11/22/2016 - SHRM)



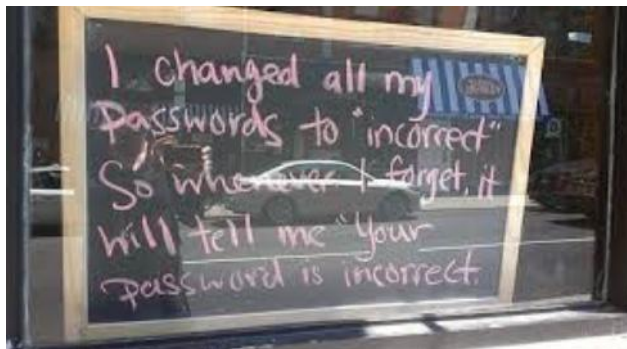
## Bottom Line:

Get serious  
about protecting yourself  
against cybercrime!

*But what does that look like?*



## W3@k Pa55w0rd5




## So How Do You Protect Yourself?




# Stay Up to Date

- Learn about Big Data
- Data analytics
- Mobile devices
- IoT


# Review HR Processes (Vulnerable Moments)

- Recruitment
- Onboarding
- Status changes
- Termination
- IoT / Tools




# AUP

- Acceptable Use Policy
  - Guidelines for use of technology in the workplace
  - Promotes computer & online safety
  - Sets clear expectations
  - Removes ambiguities
  - Puts it in writing



# Alaska 45.48.010

State Statute	What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exception or safe harbor?	Enforcement? Penalties? Is there a private right of action?
Alaska Stat. §45.48.010 et seq.	<b>Covered entities:</b> "Covered person" who "owns or licenses personal information in any form that includes personal information on a state resident" (§45.48.010(a)).  "Covered person" defined as " (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees." (§45.48.000(2)).  <b>Service provider requirement:</b> "Yes" if a breach of the security of the information system containing personal information on a state resident that is not required by an information recipient occurs, the information recipient is not	<b>Personal information:</b> "If information is any form on an individual that is not encrypted or redacted, or is intercepted and the recipient key has been assumed or obtained, and that consists of a combination of: (A) an individual's name, in this subparagraph, "individual" means: (i) first name or first initial, and (ii) last name; (B) one or more of the following information elements: (i) social security number; (ii) driver's license or state ID card number; (iii) date of birth; (iv) individual's account number, account number, credit card	<b>Breach definition:</b> "A breach of the security" means "unauthorized acquisition, or possession, or use of unauthorized acquisition, or personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector." (§45.48.000(1)).  "Acquisition" includes acquisition and: (i) photocopying; facsimile, or other page-based method; (ii) a device, including a computer, fax machine, or other information that is represented in numerical form, or (C) a tracked card identified by (A) or	<b>Resident:</b> "If a state resident whose personal information was subject to the breach." (§45.48.000(a)).  <b>Credit reporting agency notice requirement:</b> Yes, "to notify every resident of a breach, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on nationwide basis and provide the agencies with the listing, distribution, and content of the system to state residents." (B) This section may not be construed to require the information collector to provide the consumer reporting	<b>Timing:</b> "An information collector shall make the disclosure required by ... this section in the most expeditious time possible and without unreasonable delay, except as impacted by law enforcement) and as necessary to contain the scope of the breach and reduce the potential integrity of the information system." (§45.48.010(b)).  <b>Delay:</b> "An information collector may delay disclosing the breach ... if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation." However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without	<b>Method:</b> "An information collector shall make the disclosure required by AS 45.48.010 (1) by a written document sent to the most recent address the information collector has for the state resident; (2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means or if mailing the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for records legally required to be in writing under 15 U.S.C. 2081 et seq. (Electronic Signatures in Global and National Commerce Act); or (3) if the	<b>For enabling law enforcement:</b> No.  <b>For following emergency guidance:</b> No.	<b>State enforcement:</b> "If an information collector ... violates AS 45.48.010 (1) or (2), the information collector is not subject to the civil penalties provided under AS 45.50.051 but is liable to the state for a civil penalty of up to \$100 for each state resident who was not notified under AS 45.48.010 (1), \$500,000, except that the total civil penalty may not exceed \$10,000,000." (§45.48.000(3)).  <b>Private right of action:</b> Yes. Alaska residents



## Tips For Protection:

- Cancel employee debit cards
  - the #1 way bank accounts get compromised
- Have a dedicated PC for online banking/compensation & DON'T use that PC for accessing any other web sites, e-mail access, social media sites or for downloading files & applications
- Sign up for e-mail alerts for transactions on bank & credit cards
- Require the appropriate signature for any wire transfers
- Use multiple bank accounts to minimize the risk



## Cost Effective Solutions

- Keep your Operating System up to date
- Use & keep current your Anti-Virus
- Know what's running on your network
- *Back up your data*
- Use a password app
- Learn how to read an email or web link
- Use protected DNS
- Be skeptical of unsolicited advice
- Train employees & contractors
- Use professional support
- Cyber insurance



## Computers Under Control!

- To remove files that live in your computer:
  - <https://www.piriform.com/ccleaner/>
  - Creators of CCleaner, Defraggler, Recuva & other tools—all of which have free versions
- To clean up malware, spyware, & adware:
  - <https://www.Malwarebytes.com>
- Safe software downloads:
  - <https://download.cnet.com>



## Info Lookups

- <https://haveibeenpwned.com/>
- <https://www.knowbe4.com/email-exposure-check/>
- <http://www.linkexpander.com/>
- <https://www.bleepingcomputer.com/>
- <https://www.google.com/>



### 3 Steps To Protecting Your Organization:

- **Step 1: Threat Assessment**  
What do you have that needs protection?
- What is the state of your current IT environment?
- **Step 2: Action Plan**  
What can be done to better protect yourself now?
- **Step 3: Ongoing Maintenance**  
You definitely don't want to take a "set-it-and-forget-it" approach to security – your attackers aren't!



### Our Basic Recommendations

- **A Layered Approach to Security**
  - Network level protection
  - Data level protection
  - Email virus & spam filtering
  - **Mobile Device Management**
  - Application & patch management
  - Workstation protection
  - **User training**
  - **Effective business policies**



### Know Your Profile

We will conduct a "Threat Assessment" at your office where we will:

- Collect a baseline of your information
  - "second opinion"
- Know what's running on your network
  - Often neglected
- Discuss our findings with you
  - In-depth reports
- Provide a roadmap for your business going forward



### Questions



Thank you!

**DanTech Services**

907-885-0500

[www.dantechservices.com](http://www.dantechservices.com)

