

# SECURITY AWARENESS: A BLUEPRINT FROM START TO FINISH-ISH

---

**SÜDDEUTSCHE ZEITUNG**

How much data are we  
talking about?

**JOHN DOE**

More data than anything  
you have ever seen.



PANAMA PAPERS

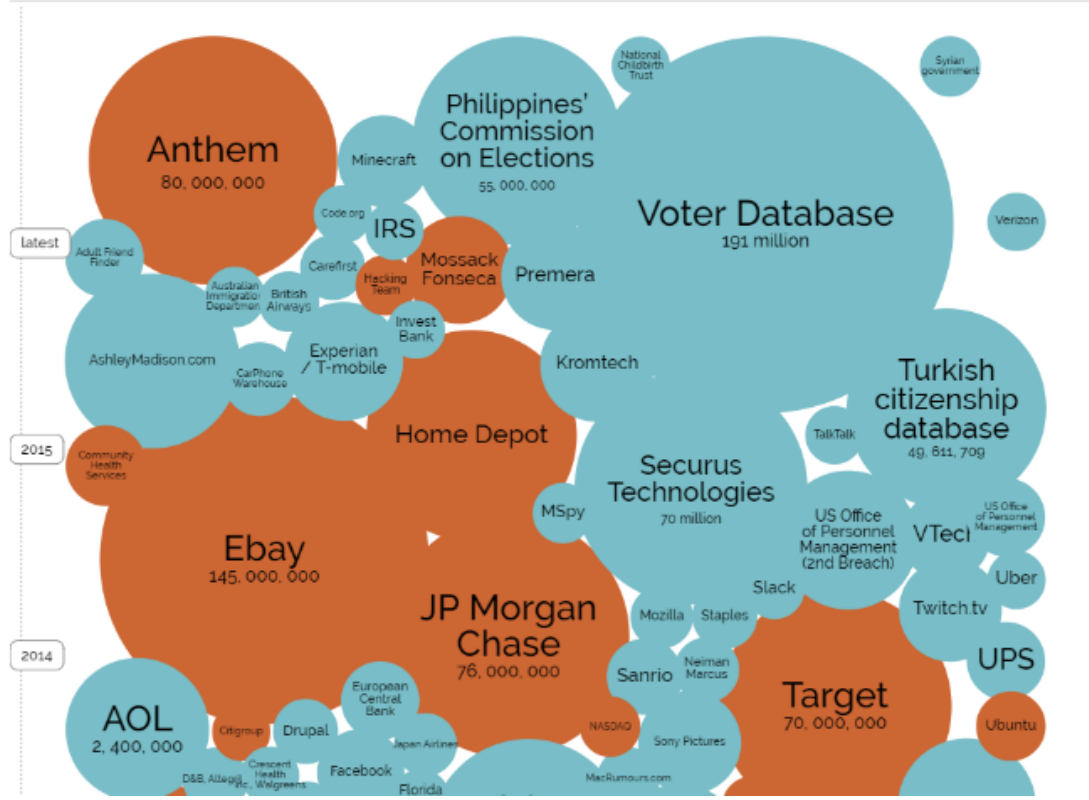
# World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 6th May 2016)

interesting story

YEAR BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY SHOW FILTER



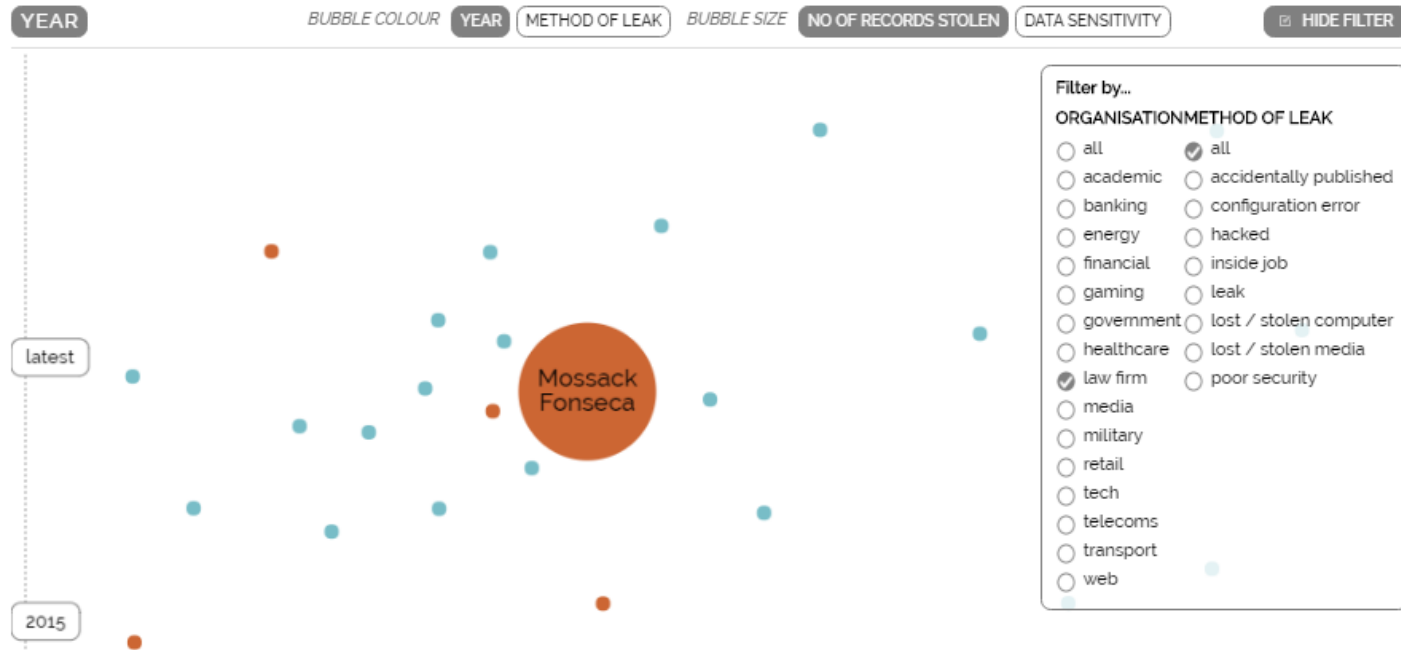
# World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 6th May 2016)



interesting story



ILTA CON 2016

# The size of the Panama Papers leak

Amount of data compared to previous leaks



Source: International Consortium of Investigative Journalists (ICIJ)

BBC



ILTA CON 2016

# STRATEGY 1: DESIGN FOR **THE LONG HAUL**

---

This isn't a rollout project. You don't get to "done."

# Design for **the long haul**

- Compliance or change?
  - How often is often “enough”?
  - Feed the beast
  - Balance the load
  - Get creative...for their sake and yours
-





Check the box...or change behavior?



**Organizations** don't change.  
**People** within organizations change.





The background features a repeating pattern of black brushstrokes on a light gray background. Each stroke consists of a horizontal line with several vertical lines extending downwards from it, resembling a stylized 'H' or a comb. The strokes are slightly blurred and vary in focus, creating a sense of depth and movement.

How often is often **enough**?

Strong Passwords

HIPAA

Social Engineering

Mobile Devices

Ransomware

Phishing

The Cloud

Environment

Telephone scams

Public WiFi

USB Use

Paper-based data



packers #1

**NUMBER OF TRIES TO GUESS HIS PASSWORD: 3**

**HOW MANY WOULD IT TAKE TO GUESS YOUR PASSWORD?**

**nGuard**  
Work safe. Know how.  
Security Awareness Program



## Creating Smart Passwords

What is a "smart" password? A smart password strikes a balance between being **easy-to-remember** and **hard-to-guess**. The best practices below will help you create smart passwords, but remember to refer to your firm's password policy for specific guidance on the number of characters required and any restrictions to keep in mind.

### Easy-to-Remember

**Step 1** Instead of using a password, create a passphrase. For example, sink or swim or once upon a time. To make it easy to remember, choose a passphrase that has personal meaning for you but isn't something that could be easily guessed by walking into your office.

### Twist and shout

Once you've chosen a passphrase, use letter substitutions to incorporate numbers, capital letters, and special characters into your passphrase. Remember to refer to the requirements specifically for your organization's policy.



## Why all the talk about security?

**cy-ber at-tack** [sahy-ber-uh-tak]  
noun  
an attempt to damage, disrupt, or gain unauthorized access to a computer, computer system or electronic communications network.

Also, cyberattack.



President Obama addressed the increasing threat of cyber attacks during his State of the Union Address, February 22, 2013.



ILTA CON 2016



Feed the beast





PANAMA  
PAPERS



MOSSACK  
FONSECA





🔑 Pension Funds  
Pile on Risk Just to  
Get a Reasonable  
Return



🔑 Stocks Mixed, But on  
Track for a Winning  
May



🔑 Judge Finds  
Michael Dell, Silver  
Lake Underpaid for  
Dell in 2013

**MARKETS**

🔑 Goldman Loans \$75 Million to IPO  
Hopeful Nutanix



🔑 Barc  
Charged  
Passing



**YOU ARE READING A PREVIEW OF A PAID ARTICLE. [SUBSCRIBE NOW](#) TO GET MORE GREAT CONTENT.**



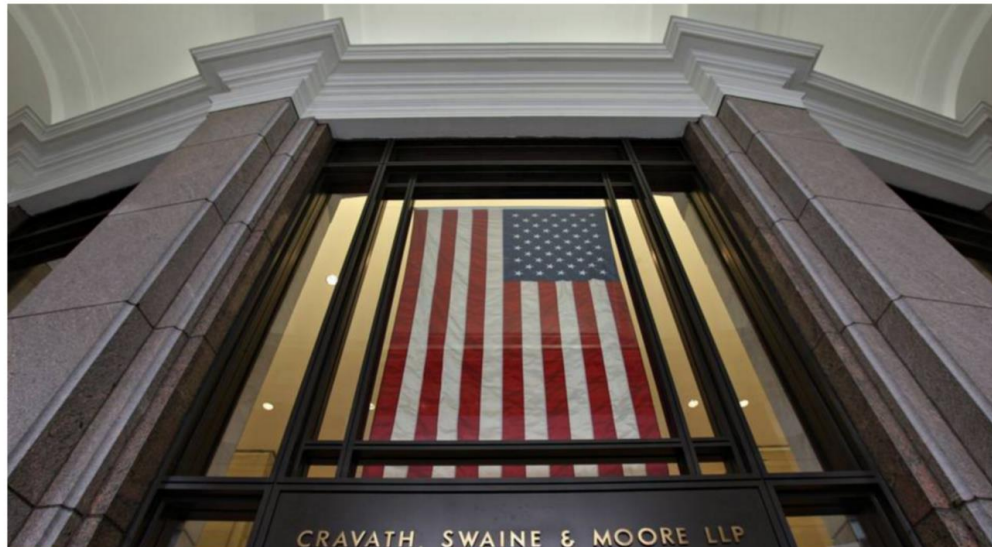
522



**MARKETS**

## Hackers Breach Law Firms, Including Cravath and Weil Gotshal

Investigators explore whether cybercriminals wanted information for insider trading



Thanks for the feedback! [Undo](#)

We'll use your feedback to review ads on this site.

Help us show you better ads by updating your [ads settings](#).

OnGuard™ Daily

OnGuard Members

## Cyber Security

View on Site [News](#) (281) [Tweets](#) (190)

Companies Mentioned Most

• [Active Network](#) • [Financial Institutions](#) • [Share](#) • [Insightly Inc](#)

### [Illinois strengthens, expands scope of personal information protections](#)

June 2nd at 3:47 AM in the Thompson Coburn Publications

... Thompson Coburn's Cybersecurity Department.

### [eAlert Cybersecurity Implications of Supreme Court's Spokeo Decision Begin to Emerge \(June 2016\)](#)

#### In This Alert

##### Topics

[Cyber Security](#) (5)  
[Data Breach](#) (5)  
[Information Governance](#) (2)  
[Risk Management](#) (5)  
[Security Audit](#) (1)  
[Security Awareness](#) (4)

##### Practices

[Data Privacy](#) (5)  
[HIPAA](#) (5)  
[HITECH Act](#) (2)  
[ISO 27001](#) (3)



A hand at the bottom left holds a thin, light-colored stick vertically. At the top of the stick, a bright red plate is balanced perfectly. To the right, another hand is raised, palm facing forward, with fingers slightly spread. The background is a clear, light blue sky. A semi-transparent white banner is positioned horizontally across the middle of the image, containing the text "Balance the load".

Balance the load

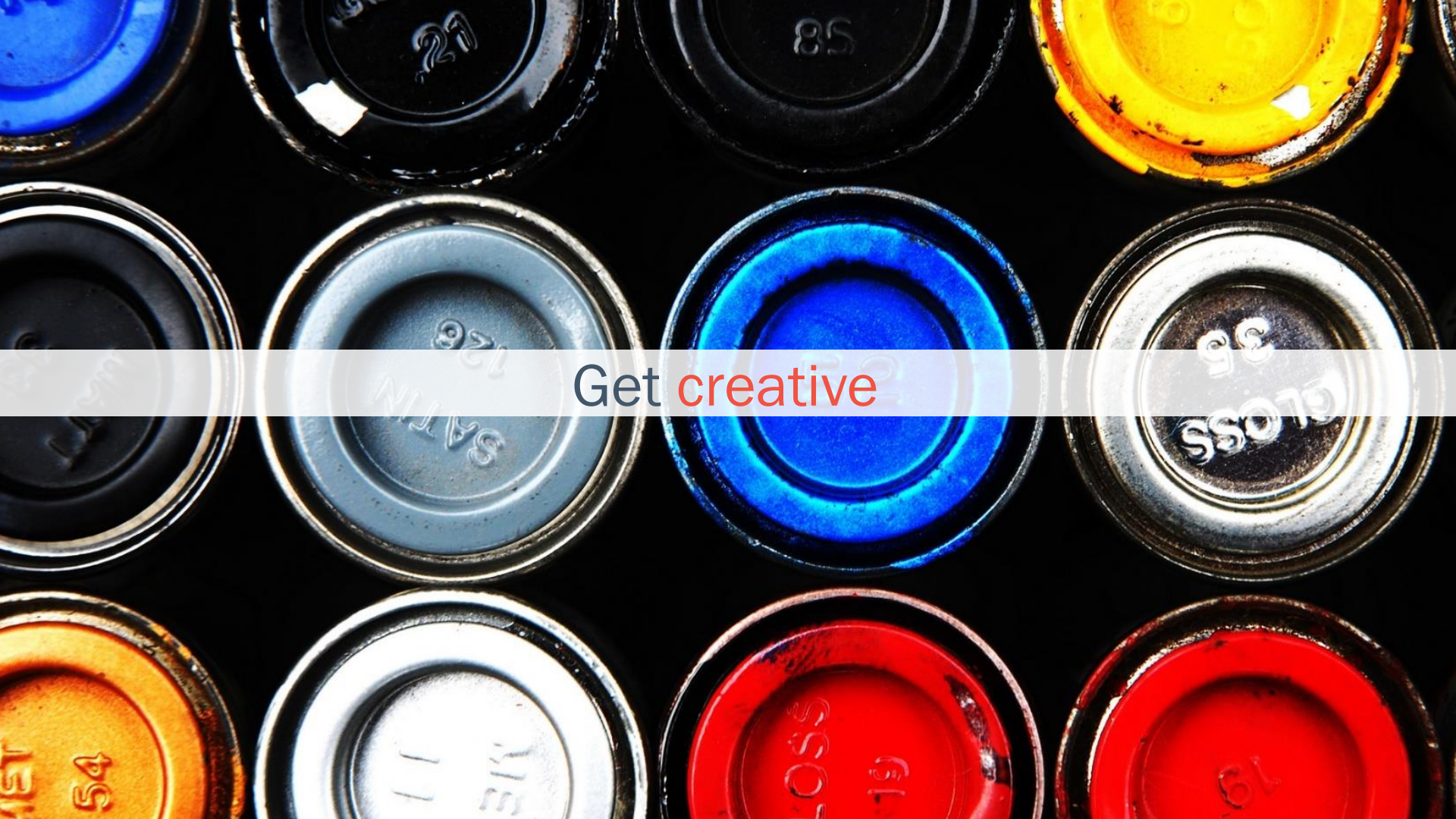




You need a hero...maybe even a few

- 
- A group of people in superhero costumes at a convention. In the foreground, a man is dressed as The Flash in a red suit with a yellow lightning bolt on his chest. To his left, another man is dressed as Green Arrow in a green suit with a white arrow on his chest. In the background, other people are dressed as various superheroes, including Batman and Wonder Woman. The scene is set in a large, brightly lit indoor space, likely a convention hall.
- COO/Managing Partner
  - Practice Group Leaders
  - Department Heads
  - Key influencers in the Firm





Get creative





Get creative with **Delivery**



What's keeping  
your firm from  
becoming a  
statistic?





Get creative with **Resources**

SOPHOS

## THREAT HUNTER



See how many security risks you can identify on this messy desk in 30 seconds

PLAY

AARP Foundation

Search



ED GRANTS FIND HELP WAYS TO GIVE

MORE FROM AARP

Legal Advocacy

Income » AARP Foundation ElderWatch » Recognize Fraud

## ation ElderWatch

CAUTION



Report fraud or financial exploitation.

1-800-222-4444, option 2

Hacker leaks millions of Hotmail, Gmail, and Yahoo Mail usernames and passwords

## RAISING DIGITAL CITIZENS

Teach your children to become good digital citizens.



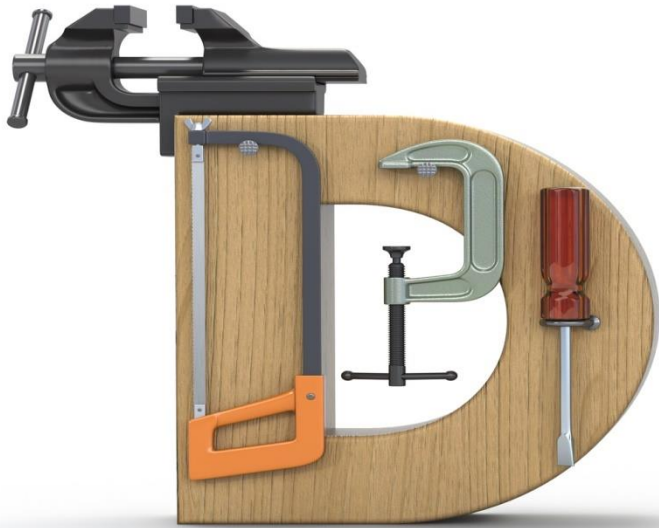
Get creative with **Incentives**

# STRATEGY 2: DESIGN FOR **DIY**

---

Building an effective Security Awareness program in-house





# Who Should Present?

- CIO / IT Director
- CISO (If they are not human friendly don't force it)
- 1-2 Attorneys (HIPAA / IP / Technology Focused)
- Guest Speaker (FBI or Local Police Liaison)
- Managing Partner Buy-In & Support is Critical
  - They should send the invitation/appointment
  - Stress the importance of attending (mandatory?)
  - Kick off the session & introduce the speakers
- Make the session slightly general  
(i.e. not too firm specific) = CLE
- Combine with Annual HIPAA Training Requirement

# Guest speakers make it interesting and REAL (\*they are also Free\*)

- FBI or Local Infragard Chapter (plan in advance)
  - They cover cyber terrorism and criminal activity
- Local Police Departments typically have a liaison
  - Active Shooter Discussions are difficult, but necessary for most law firms. Develop a physical security plan.
- Other Local Experts can validate what you say – but be sure to vet their slides and messaging
- Keep all guest speakers to a strict time-limit or else they could eat up the entire session time.
- Save all audience Q&A until the end (time crunch)



# Timing is Important

**1x per year (min)**

**60-90 min (max)**

**Afternoon (not lunch)**





# Format?

**Live Presentation  
w/WebEx or Zoom Broadcast**

**Record for Replay  
& New Hires (mandatory)**



# What to Cover?

- (1) PREVENTION**
- (2) DETECTION**
- (3) RESPONSE**
- (4) RECOVERY**

# PREVENTION

Hardware

Software

Data

Procedures

People

## Technical Safeguards

Identification and authorization  
Encryption  
Firewalls  
Malware protection  
Application design

## Data Safeguards

Data rights and responsibilities  
Passwords  
Encryption  
Backup and recovery  
Physical security

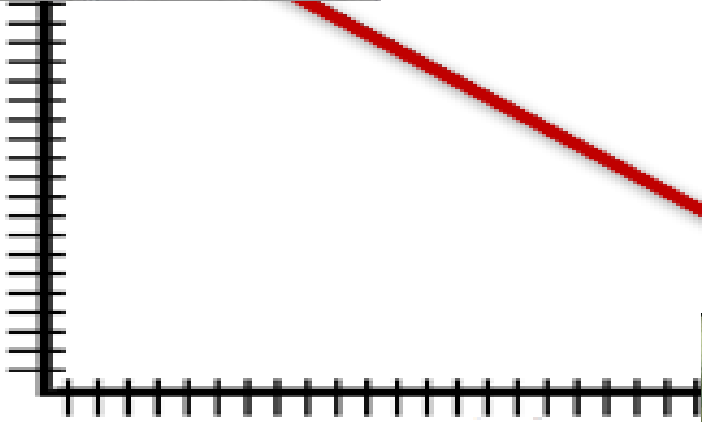
## Human Safeguards

Hiring  
Training  
Education  
Procedure design  
Administration  
Assessment  
Compliance  
Accountability



# PREVENTION - INFOSEC IS A BALANCE BETWEEN USABILITY & SECURITY

Level of  
Usability or  
Functionality



Level of Security



# Physical Security

- Office Nameplates & Light Switches have the office number on them & Light Switches have building security contact #
- In an emergency situation, call 911, pull the fire alarm, push/pull the blue panic button in the corridors – Help will be on the way
- Even if you can't speak, call 911 leave an open line
- Front Desk has a silent panic button that alerts the building security office and the Milwaukee Police Department
- Run / Hide / Fight <https://www.youtube.com/watch?v=5VcSwejU2D0>

# Vendors/Contractors in Our Space

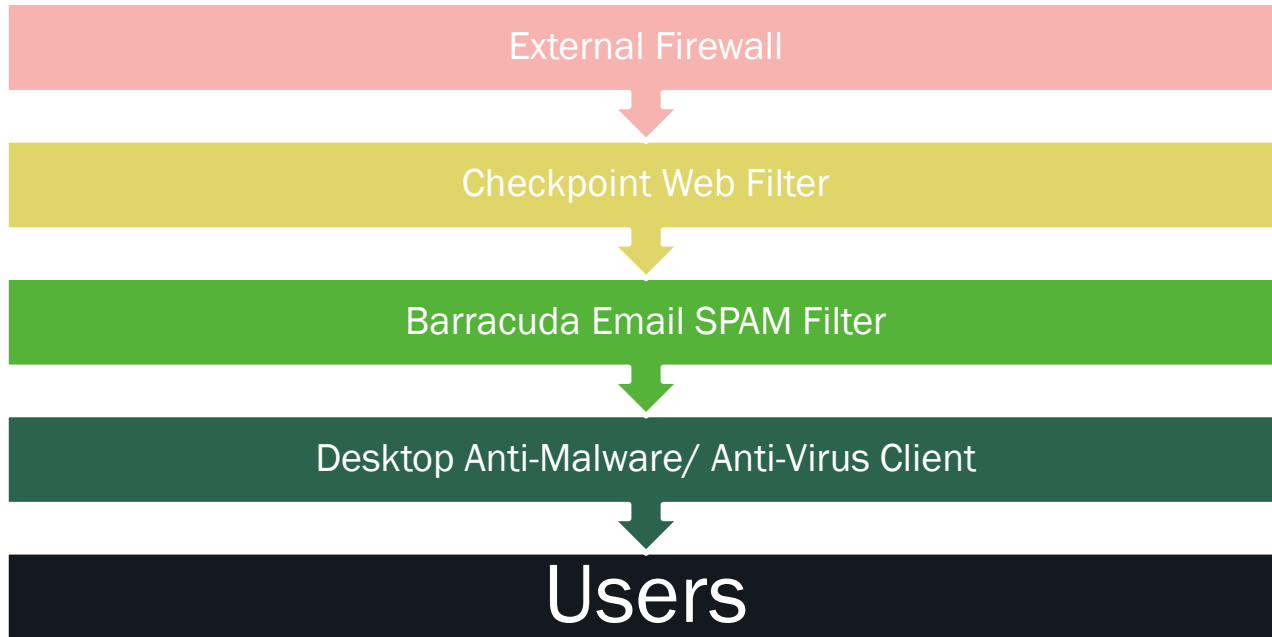


If you don't know someone, ask:  
**Who are you? Why are you here?**  
Call Reception or Call Support Services/IT  
For Backup

# Safeguards

- Firewalls / 2FA / Multi-Vendor Approach / Sensors / Logs
- Laptop/Desktop Endpoint Utilities & Scanning
- Mobile Phones/Tablets: Never leave unattended in a public setting
- Don't let kids/family members play games on work devices
- Copier Fleet – Swipe Your ID Badge to Use
- Non-employees will not be able to scan/copy
- Secure Print Feature on Copiers & Printers – Print Job can be held in a secure state and printed when you arrive at the device

# Multi-Tier Information Security





# PREVENTION

## Browser Links & Links in Email Hover Over to Visually Verify

From: "Link  
Subject: Ne  
Date: Octob  
To: <info@o

The screenshot shows a Google search for "jet airways". The search results page displays several links and an advertisement. A mouse cursor is hovering over the link "jetairways.com - Cheap Flight Ticket India" in the advertisement. A callout box highlights the URL "www.jetairways.com/". A green arrow points from the text "on hover over link" to the callout box. The search results include:

- Ad related to jet airways: [jetairways.com - Cheap Flight Ticket India](#) (www.jetairways.com/). Book flight tickets, hotels India's finest international airline!
- Jet Airways | Book Flight Tickets, Hotels Online on this Airline... (www.jetairways.com/). Jet Airways - India's finest international airline and one of the fastest growing airlines in the world is all set to change the way you fly - for the better! We operate ...
- India: Jet Airways India - one of the fastest growing airlines in the ...
- Book Online: Cash on Delivery. Cash on Delivery. Jet Airways introduces ...
- Web Check-in: Web check-in service at jetairways.com reduces your waiting
- PNR Status: All guests who are traveling with Jet Airways can check the real ...
- United Kingdom (UK): Book Online - Flight Information - JetPrivilege Login - ...
- United States of America: Contact Us - Flight Status - Flights - Baggage - PNR Status - ...
- Super Cheap Flight Rates: www.lowfares.com/Cheap-Flights. Hundreds of Fares to Choose From. Compare Now to Get the Best Deal!
- Book Flights To Bangkok: www.makemytrip.com/Bangkok-Flights. Book Cheap Flights to Bangkok. Quality Service. Book Now & Save! 162 people +1'd this page
- Jet Flight Coupon Codes: www.desidime.com/jetairways-coupons. Great Discounts on Flight Booking. Apply Coupon to get Rs. 500 Off
- Fly Virgin Atlantic: www.virgin-atlantic.com/. Excellent Air Fares on London Flights. Book Online Now!

It

t

# PREVENTION

## USB Thumb Flash Drives

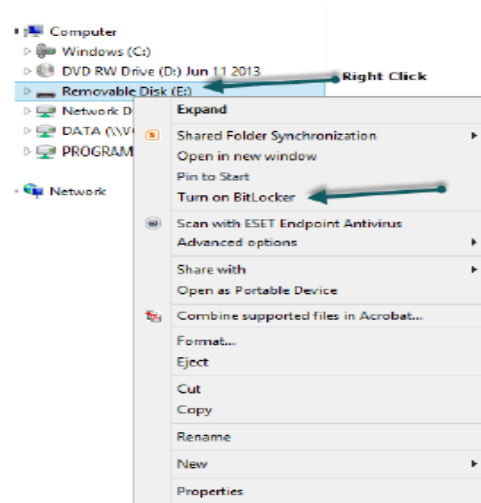


### Steps to encrypt your USB Drive:

1. Insert the USB flash drive; click the file folder in the task bar to see the drives on your computer.



2. Right click on the USB flash drive; Click **Turn on BitLocker**.



# Cell Phone Charging Kiosk A Hacker's Dream



## PREVENTION

# Do Not Use Work Email for eCommerce/Shopping/Banking

- Automatically delete all banking/shopping/ecommerce emails without a second thought because your work email is only for work
- Most people use the one email address across all sites – identity theft
- Create unique email addresses/accounts for each site
  - [bcaraherAmazon@gmail.com](mailto:bcaraherAmazon@gmail.com) --pass: Sh0pping098books!
  - [bcaraherBMO@gmail.com](mailto:bcaraherBMO@gmail.com) –pass: Sh0pping098banking!
  - [bcaraherGap@gmail.com](mailto:bcaraherGap@gmail.com) --pass: Sh0pping098clothes!

If you have multiple online identities, it will be nearly impossible for someone to hack your life!


FBI DOES NOT RECOMMEND LASTPASS or PASSWORD APPS  
THEY HAVE BEEN HACKED TOO!



## PREVENTION

# Recent Email Phishing Scams

From: Brooke Rodriguez <shane@truehealth4life.com.au>  
To: Michael P. Carlton  
Cc:  
Subject: Brooke Rodriguez

Message  755\_b217\_i9-kfekv.rtf (239 KB)

Greetings

See the document in attachment. To eliminate additional costs you have to pay in next 24 hours.


Regards

Brooke Rodriguez

**These types of email  
Scams are only going to get  
better and more targeted.**


**From: Randy Crocker**

**From: PGL, etc.**

 You forwarded this message on 5/2/2016 11:57 AM.

From: Lee, Jason <JALee@federalsignal.com>  
To:  
Cc:  
Subject: IT Service Center

Sent: Mon 5/2/2016 11:57 AM

Message  IT Service Desk.pdf (186 KB)

This Message is from Helpdesk Administrator. Please read attach message and follow instruction accordingly.



**!!!SET GOOD POLICIES!!!**

**EMAIL FROM: HELPDESK@VONBRIESEN.COM  
WILL NEVER SEND YOU LINKS, DOCUMENTS  
OR REQUESTS**

**ALSO DO NOT ENTER YOUR USERID  
OR PASSWORD IN AN EMAIL  
OR A WEB BASED\ONLINE FORM**

# Email Scams for Representation

From: Kaga Electronics Co Ltd <kagaelectronics@asia.com>  
To: Bill Caraher  
Cc:  
Subject: litigation case

Sent: Wed 4/23/2014 4:00 PM

This is a request for your legal consultation services, I would like your advice regarding possible representation on a litigation case concerning breach of contract/collection matters. I believe that the matter is within your jurisdiction which is why I'm requesting your legal advice. After a careful review of your firms profile as well as your qualification and experience, we are of the opinion that you are qualified to provide the legal services as requested.  
Do let me know your position in reviewing this matter, so I may provide any additional information. I look forward to your prompt response.

Regards,  
Tomohisa Tsukamoto  
CEO and President  
Kaga Electronics Co., Ltd  
2-8, Sotokanda 3-chome,  
Chiyoda-ku, Tokyo 101-8629 Japan

# von Briesen Website Disclaimer

## Disclaimer

The contents of this web site are for informational purposes only and are not intended as legal advice. Materials on this web site are current only as of the date when they were originally published. Legal advice will only be given after an attorney-client relationship has been established pursuant to the firm's policies and procedures, and then only in reference to a client's specific circumstances. You cannot create an attorney-client relationship with us by reviewing information on our web site or by communicating with us by electronic mail or other means. If you are interested in seeking to establish an attorney client relationship with a lawyer in the firm please call that lawyer directly; otherwise you can telephone the practice group leader of the group which handles your type of legal issue. An attorney-client relationship will be established only after we have determined that we have no conflicts of interest that would prevent us from representing you, and you and the firm have reached an agreement setting forth the terms of our representation. If you do not have an attorney-client relationship with us, your communications with us via electronic mail or some other means may not be privileged. Usually we will not enter into an attorney-client relationship that requires the performance of legal services in a jurisdiction where we are not licensed to provide such services. A listing of jurisdictions where our attorneys are licensed to practice law can be found on each individual attorney's biography.



# Scammers are Targeting Us

**Xymox Technologies Inc**  
9099 W Dean Road  
Milwaukee, WI 532242852

The Bank of Nova Scotia  
Station Place D'Armes  
Montreal, QC H2Y 3E9

59438

DATE 09 10 2015  
MMDDYYYY

PAY \*\*\*THREE HUNDRED FIFTY THOUSAND AND 00/100 US DOLLARS\*\*\*

\$\*\*\*350,000.00USD

TO THE  
ORDER  
OF

von Briesen & Roper, s.c.  
411 East Wisconsin Avenue, Suite 1000  
Milwaukee, WI 53202

Memo: Star Micronics

PER 

PER 

⑈059438⑈ ⑆47696⑆002⑆ 06223⑆11⑈

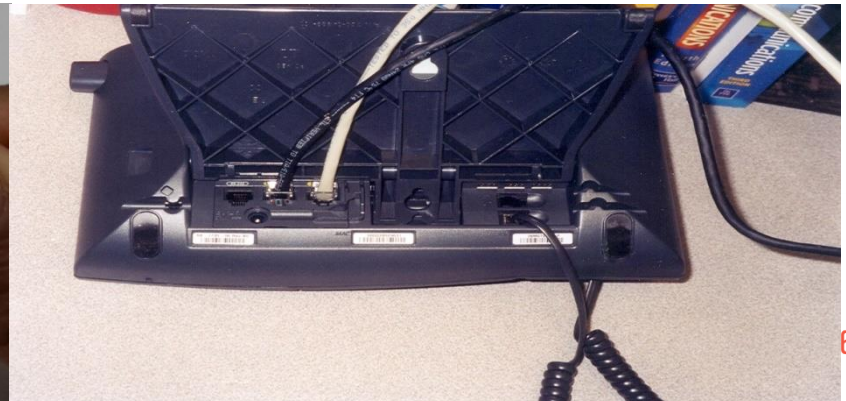
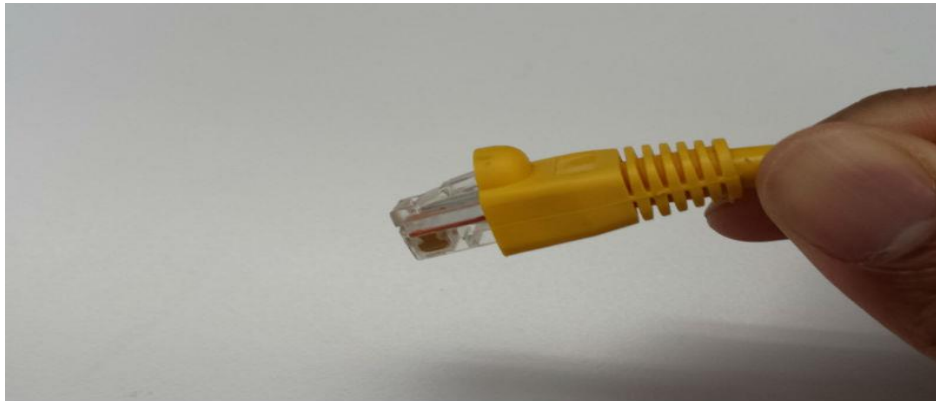


ILTACON 2016

## RESPONSE

# If Your Machine is Acting Weird or You Clicked/Opened Something Bad

- 1) Close the App/Browser
- 2) Close the Lid/Turn Off Your System (Try to quickly save work first)
- 3) Pull Out Your Network Cable / Turn Off WiFi / VPN





# RESPONSE

homeoknow.com says:

**\*\* YOUR COMPUTER HAS BEEN BLOCKED \*\***

Error # 268D3

Please call us immediately at: 844-576-0492

Please do not ignore this critical alert. If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen...

- > Facebook Login
- > Credit Card Details
- > Email Account Login
- > Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: 844-576-0492

Prevent this page from creating additional dialogs.

OK

Typo - <http://youtuber.com>

# SMS TEXT SCAMS

# VOICEMAIL SCAMS

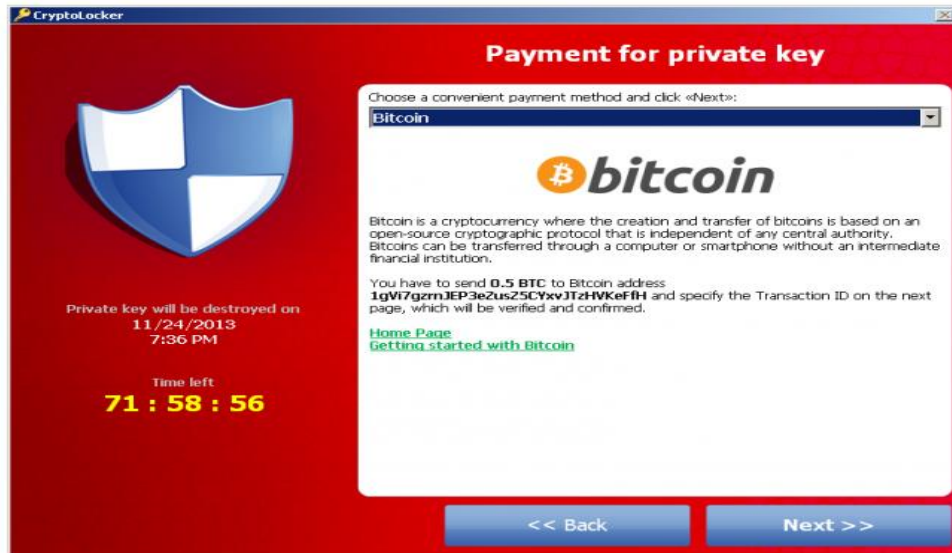
# USPS SCAMS



# RESPONSE / RECOVERY

## Ransomware is a very real threat.

- Notify IT immediately if it happens to you
- Unplug from Network / Turn Off Immediately
- Do not store client data, originals or other irreplaceable work product on your computer



- Don't store personal data (pics/music/docs) on vB PC
- We will wipe computer if infected w/ransomware
- FBI Says: Never pay the ransom



ILTACON 2016

State-sponsored	The Actor or group is employed by the government of a nation-state.
Individual	A specific person or group acting on their own, and not a member of any other Actor threat category.
Hacktivist	An actor that performs attacks in order to draw attention to a cause (such as free speech or human rights), or hinder the support of a cause. If the cause is political, and/or designed to inflict terror, they are instead considered a Cyber terrorist.
Cyber terrorist	Actor carries out an attack designed to cause alarm or panic with ideological or political goals. Alternatively, if the actor is party to a known terrorist organization.
Organized Crime	Groups of criminals that intend to engage in illegal activity, most commonly for monetary profit. Attacks are designed to either extort money from the target, or the actors are funded to carry out an attack.
Identity Unknown	Actor is not identified within the document, either by handle or affiliation.
Organization	Organizations not specifically associated with information security but having some affect over the information security space.
Information Security	Includes organizations or persons from, or whose actions affect, the Information Security sector. These are security researchers, computer scientists, antivirus vendors, CERTs, threat intelligence (non-state-sponsored).
Law Enforcement/Authority	Will include anyone involved in law enforcement (police, police cyber crime units, courts, judges) as well as attorneys and lawyers.



# Threat Actors



<https://www.surfwatchlab.com/threat-categories#Actor>

# Protected Health Information (HIPAA)

Health Insurance Portability and Accountability Act of 1996

The Health Information Technology Economic and Clinical Act (Title XIII of the American Recovery and Reinvestment Act of 2009)

PHI is individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

- PHI Excludes
  - Employment records maintained by covered entities in their capacities as employers; and
  - Education and other records subject to the Family Educational Rights and Privacy Act



# What Makes Information Identifiable?

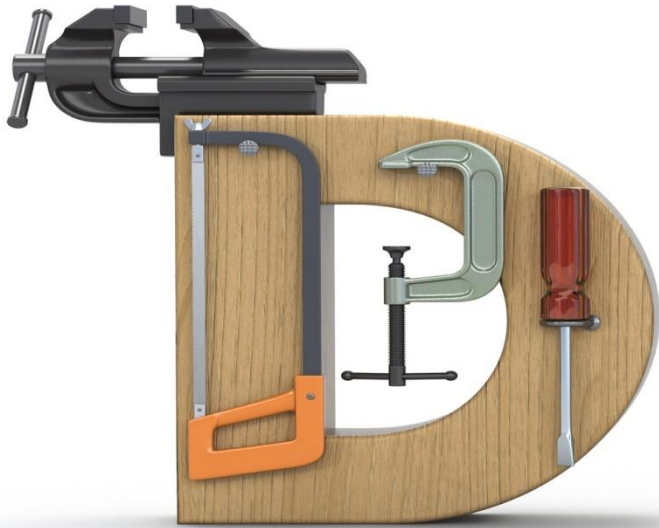
1. Name
2. Address (geographic subdivisions smaller than a state)
3. Email address
4. Dates (except years)
  - Birth Date
  - Admission/Discharge Dates
5. Telephone numbers
6. Fax numbers
7. Social Security Number
8. Medical record number
9. Health plan beneficiary number
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (not the unique code assigned by the investigator to code the data)

**All 18 elements must be removed for data to be “de-identified”**  
**Note: Generally, redaction is not sufficient to de-identify PHI**

# When Do We Have to Comply?

When we create, receive, maintain or transmit PHI when representing:

- A “covered entity”
  - Health plans
  - Health care providers
  - Health care clearinghouses
  - Hybrid entities (e.g., municipalities)
- A “business associate” or other entity that supports the health care industry



# SECURITY AWARENESS: A BLUEPRINT FROM START TO FINISH-ISH

---

## QUESTIONS