

**2020
CEO
FORUM**

Don't Get Hacked – Best Practices in Cyber Hygiene

Bryan Hurd, *Vice President, Head of Office – Seattle, Aon Cyber Solutions*

Moderated by **RJ Steenstra, A.A.E., IAP, ICD.D**, *President and CEO, Fort McMurray Airport Authority*





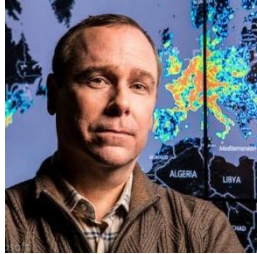
Airports Council International-North America (ACI-NA) CEOs of Airports Summit

Mr. Bryan E. Hurd – 06 Feb 2020

Bryan E. Hurd

~~CISM, CISA, CISSP, NSA-IAM, CCCI, CCFT, SNSCP~~

+ **Current: Vice President, Aon Cyber Solutions / Stroz Friedberg**



- **Director of Intelligence, Microsoft Cybercrime Center**
- **Chief of Operations, Directorate of Terrorist Identities, US National Counterterrorism Center**
- **FOUNDER US Navy Cyber Counterintelligence Program, NCIS – Naval Criminal Investigative Service**
- **Board Certified Antiterrorism Officer, U.S. Navy Antiterrorist Alert Center**



STROZ FRIEDBERG

an **Aon** company

© 2018 Stroz Friedberg. All rights reserved.

AON
Empower Results®



STROZ FRIEDBERG
an Aon company

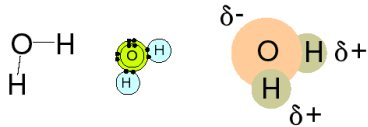
© 2018 Stroz Friedberg. All rights reserved.





Reports of significant amounts of exposure to DIHYDROGEN MONOXIDE!

- + Dihydrogen monoxide is colorless, odorless, tasteless, and kills uncounted thousands of people every year.
- + Most of these deaths are caused by accidental inhalation of DHMO
- + Dihydrogen monoxide:
 - is also known as hydroxyl acid, and is major component of acid rain.
 - may cause severe burns.
 - has been found in excised tumors of terminal cancer patients.



DIHYDROGEN MONOXIDE
A.K.A - water



ACI-NA Continuing Credit Requirement-

Exercise Number One

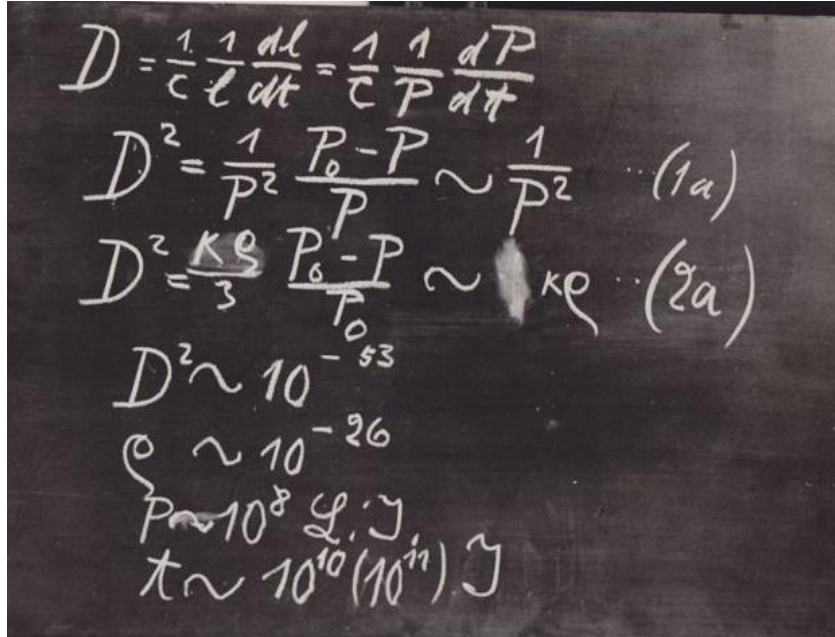
- + Please have a pencil and paper ready
 - Or do the exercise in your head if you can...

- + You will have one minute to select an option and provide an answer.....

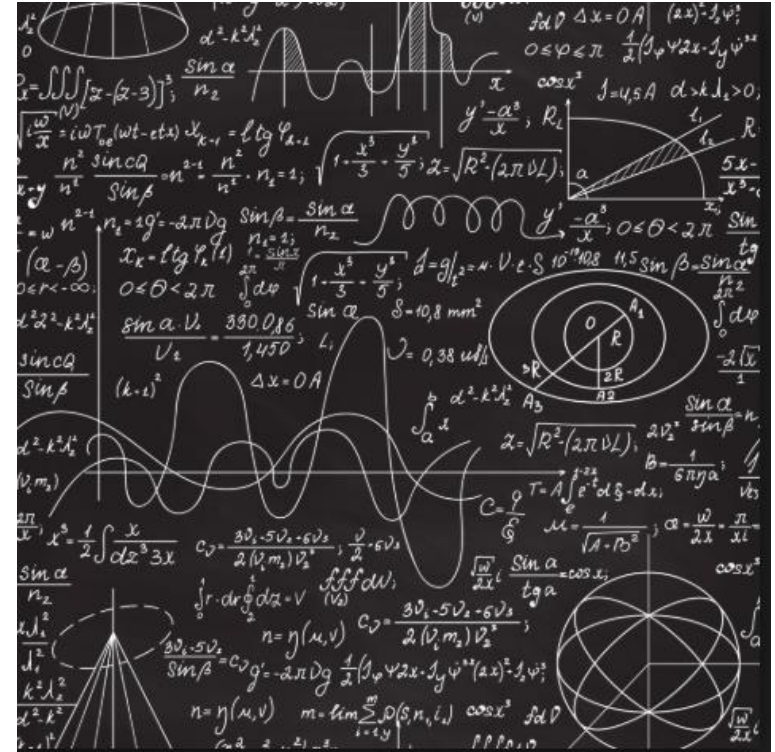
READY, SET.....

Exercise Number One – SIMPLE MATH

GO...Please solve one of these...

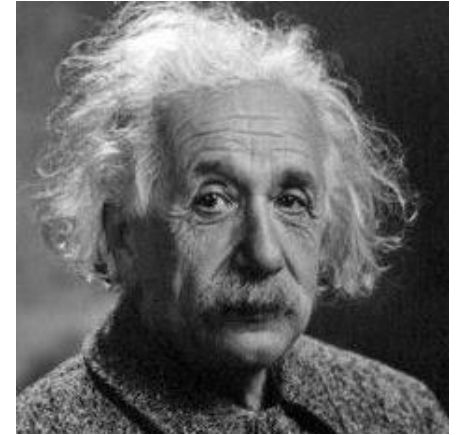


OR



Don't over complicate things...

Any Intelligent fool can make things bigger and more complex...
It takes a touch of genius – and a lot of courage to move in the opposite direction.



– Albert Einstein

Exercise Answer is

A photograph of a chalkboard with the equation $E = mc^2$ written in white chalk. The chalk is slightly smudged, giving it a realistic, hand-drawn appearance.

It is EASY to make something look COMPLEX.

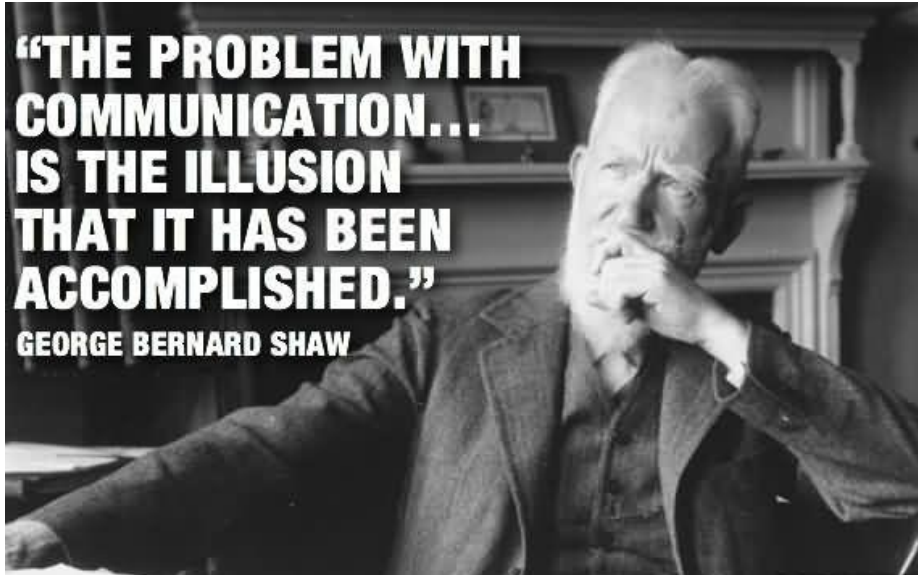


These are highly technical and highly complex issues

- Technically
- Politically
- Legally

Communication about how we work together and that we need to work together - should not be.

Communication is Key – Level It Up



- It's tempting for security professionals to focus all of their attention on the technical details:
 - Threats, Vulnerabilities, Exploits, IT Solutions, Indicators of Compromise
- + Communication about how we work together and that we need to work as a team should not be.

+ Level It Up!

The Big Intel Question - Who is the Threat?

- + **STATE:** “There are no enemies-only emerging allies.”
- + **CIA:** “We know who the enemy is, but telling you would endanger the source.”
- + **NSA:** “We know who the enemy is, but you aren’t cleared.”
- + **Director of National Intelligence** “Whomever the enemy is, we are in charge of stopping them.”
- + **US Marines:** “Doesn’t matter. Mess with the best, die like the rest.”
- + **US FBI:** “The CIA.”

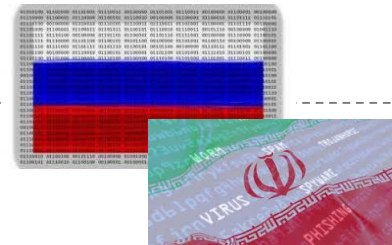




2018

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

U.S. Report - Global Issues



+ China- Theft

- sensitive trade secrets and proprietary information. It continues to use cyber espionage to support its strategic development goals—science and technology advancement, military modernization, and economic policy objectives.
- APT10 continued widespread operations to target engineering, telecommunications, and aerospace industries across the globe

+ Russia –

- Decades of cyber operations, information warfare and attacks on critical infrastructure.
- U.S. Indictments against GRU officers and Internet Research Agency for hacking US elections.
- Russia learning to hide its tradecraft in common hacker tools

+ Iran

- Iranian hacker groups Rocket Kitten targets U.S. defense, OilRig targets Saudi Arabia, APT33 has targets energy sector, and Iran theft of large educational and research institutions

[https://www.dni.gov/files/NCSC/
documents/news/20180724-
economic-espionage-pub.pdf](https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf)
© 2018 Stroz Friedberg. All rights reserved.

Nation State Tools in Hands of Criminals



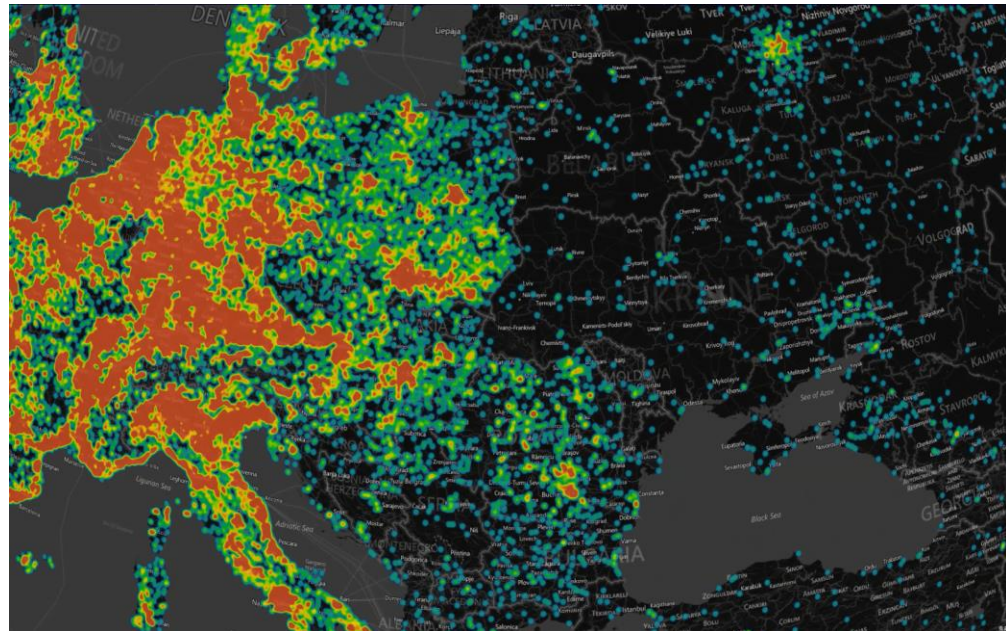
- + Shadow Brokers publish stolen NSA hacking tools from “Equation Group”
 - Supposedly NSA Tailored Access Operations (TAO)
- + Sell to highest bidder, Later posted online
- + Was the exploit behind WannaCry, NotPetya and other massive issues across the globe
- + More to be released...



Organized Crime is Going Cyber

- + Criminal groups have skilled technical staff in many areas
- + They innovate their tools and techniques with every technological era.
- + Use of digital technology to further traditional crimes
- + New cyber only crimes
- + Banking Trojans = fraud
- + Ransomware = extortion
- + DDoS protection rackets = extortion

Malware impacts are a Global Issue



Banking Trojans and SWIFT Attacks



- + \$101 Million Dollars US
- + Bangladeshi Bank
- + Malware issued unauthorized SWIFT messages AND to conceal the transfer
- + Lazarus Group = possibly North Korea
- + Dillinger quote



Attacks on SWIFT continue



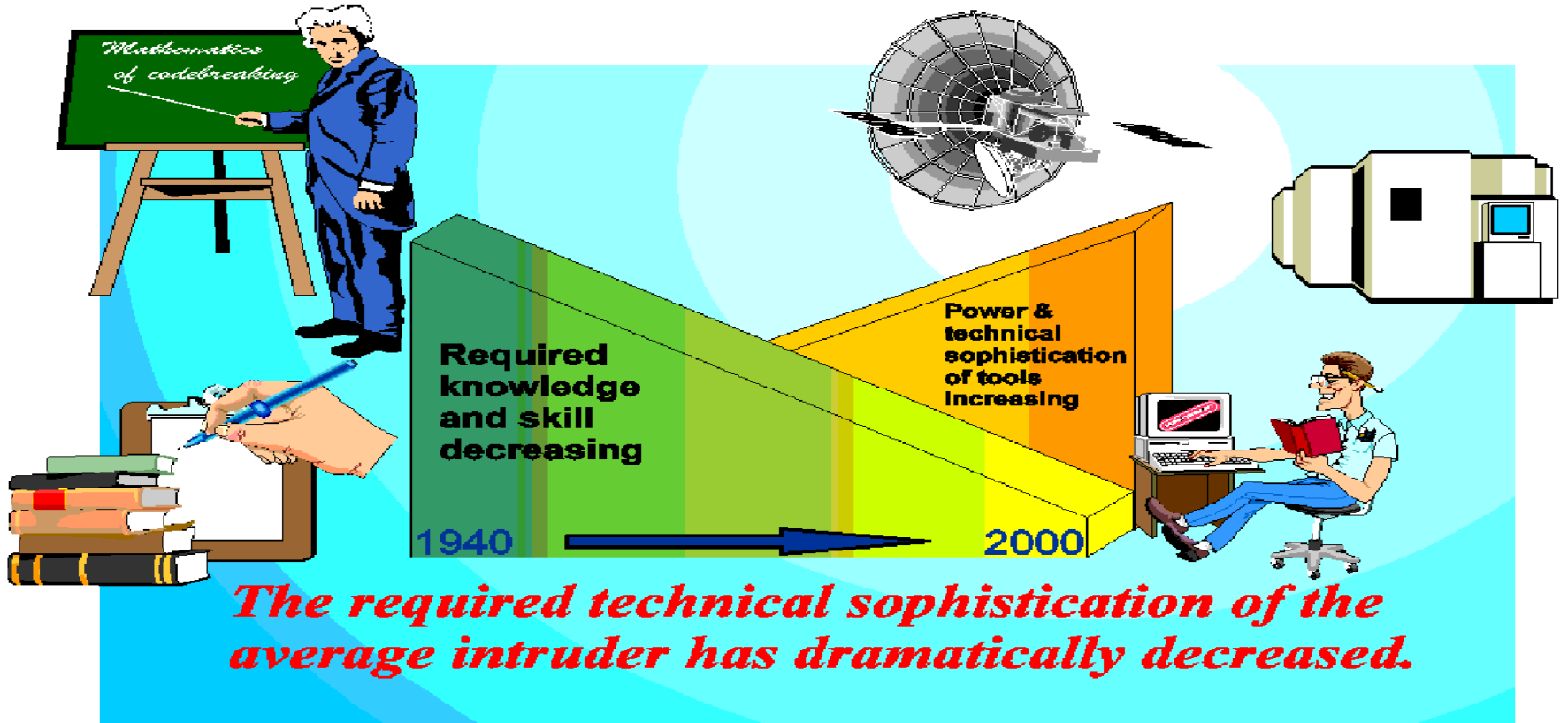
Ransomware = extortion

- Ransoms in the MILLIONS!
 - \$1.5M, \$1.7M, \$5M examples
- Ransomware hits fruit grower
 - Recovered most data, organic records lost
- Ransomware at apparel company
 - From shipping to encrypted in hours



Ransomware - cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

The HR problem in one chart... Visualization Exercise



• Outside Looking In – External Invoice Redirect

- Indicators - Proceeded by social engineering and open source info, use external email systems
- Solutions = training and processes, verification of changes

• They are Inside YOUR house – Business Account Compromise (BEC)

- Indicators - Proceeded by targeted phishing scams, email traffic redirect and use of own email systems – scams know details of travel of executives
- Solutions = email phishing training and technology, 2 factor authorization, monitoring for forwarding changes, training and processes

“The CFO Scam” – “Invoice Redirect”

Cases like this surged in the U.S. last year, with fraudsters attempting to steal a total of more than \$5.3 billion, the FBI said.



2015 - Ryanair criminal scam \$5 million (€4.6 million) taken from its bank accounts. Ryanair uses dollars to buy fuel for its 400-plus Boeing 737-800 aircraft

<https://www.irishtimes.com/news/crime-and-law/ryanair-falls-victim-to-4-6m-hacking-scam-via-chinese-bank-1.2192444>

STROZ FRIEDBERG

an Aon company

© 2018 Stroz Friedberg. All rights reserved.



Dec 2017 - Japan Airlines (JAL) email scam that cost it a not-insignificant 384 million yen (about \$3.39 million).

<https://www.digitaltrends.com/computing/email-scam-tricks-major-airline/>

AON
Empower Results®

Relevant Historical Incidents

- + **Petya Cyber Attack** – **Ransomware** which spread across **Ukraine, Britain and Spain** crippled airports and made their **systems shut down**
- + **Ataturk Airport and Sabiha Gokcen International airports** - in Turkey were targets of a coordinated attack which impacted passport control processes and resulted in massive queues and delays
- + **Warsaw Chopin Airport** – a **distributed denial of service (DDoS)** attack grounded flights when the **flight plan system** was attacked
- + **75 airports in the US** – **were attacked by an email phishing attack**, two of them had their systems compromised. The attack appeared to have **sourced from an APT (backed by a Nation State/Large Organization)**
- + **Vietnam airports - Chinese Hacking Group (1937CN)** pulled off an attack against sounds systems and information screens **Vietnam's two largest airports** and Vietnam Airlines.
- + ***All internet systems have been switched off so we had to do everything by hand,***” an airline attendant at Tan Son Nhat told Vietnam's Tuou Tre News.

Moller-Maersk – Cyber Attack Cost over \$300M

- + NotPetya - Eternal Blue and Mimikatz (credential harvest)
- + Maersk represents 18% of all container trade worldwide
- + Reckitt Benckiser reported taking an estimated £100 Million

- + Took two hours to shut down network, Staff told to go home, leaving laptops and cell phones on desks



[Source Financial Times - https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff](https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff)

Insiders are the most damaging adversaries...

Aldrich Ames betrayed more than ten top-level CIA and FBI sources who were reporting on Soviet activities, of which 4 were executed.

U.S. mole hunters investigated 90 employees- although the lead investigator noted that

"there are so many problem personalities that no one stands out".

reassigned in December 1991 to the CIA's Counter narcotics Center (CNC)

"no conscious effort was made to limit his access to classified information"



BEC - What Can FINANCE and HR and Concessions do?

- **EVERYTHING!** Ensure good CULTURE and CONTROLS
 - How can you rapidly confirm requests, especially when rank and urgency abused in BEC?
 - Are your executives “approachable” to stop abuse by criminals?
 - Will employees be supported (even rewarded) for “making a list and checking it twice”?
 - How will you communicate in a way that the adversary cannot control?
- **And have IT check for any forwarding or inbox rules on your team.**

IT and OT and IOT – Really??



- + Little or no security
- + Antiquated Operating Systems
- + Default Passwords
- + Lack of Auditing
- + Close to Day to Day Life

What a bunch of BS.... Literally....

Maroochy Shire Council waste management system - 2000

- + Sewerage control system - pumps malfunctioning, alarms were not reporting to the central computer and communication loss between the central command and pump stations.
- + Caused **800,000 liters** of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel
- + **Boden made at least 46 attempts to take control of the sewage system during March and April 2000.**
- + On 23 April, police traffic stop - found radio and computer equipment.
- + Boden's laptop hard drive contained software for accessing and controlling the sewage management system.



<https://www.sunshinecoastdaily.com.au/news/some-of-our-history-of-hacking-is-known-the-world-/3126317/>

Cyber Attack on Baku-Tbilisi-Ceyhan (BTC) - 2008

- + Massive explosion in Refahiye Turkey in 2008.
- + EXTERNAL? Infrared camera that caught two individuals with laptop computers walking near the pipeline
 - Over 60 hours of BTC video surveillance DELETED
- Hackers, probably acting under the direction of Russia, had shut down alarms, cut off communications and then super-pressurized the crude oil in the line.
- Business impact of the attack = billions of dollars.



Cyberattack 'Wake-Up Call' Puts Pipeline Industry in Hot Seat

- Companies weren't required to report attack to regulator U.S. Transportation Security Administration (TSA)
 - agency urged pipelines to take measures including establishing a cybersecurity plan, limiting network access and changing default passwords.
- Congressman sees 'bad actors' looking to weaken U.S.
- Did not interrupt flow of natural gas (Targeted I.T. systems not O.T systems)
 - Interruptions are **EXTREMELY DIFFICULT** to recover from



Held at “CYBER GUN POINT – RANSOMWARE

- + Atlanta ransomware cyberattack - \$51,000 ransom demand
 - “This is an attack on our Government, on all of us”
- + Atlanta's public-safety services such as 911, police, and fire-rescue are unaffected,



Also safe - Hartsfield Jackson International Airport systems (except WIFI)

Ransomware is hitting companies, cities and organizations all over the world.

Airports, Sea Terminals, Commercial Companies, Hospitals, Schools, Banks, Critical Infrastructure, Etc.

“Indiscriminant Targeting” of Governments, Military, Civilians,

In his own words...

- + **Fort McMurray International Airport** – A **ransomware** attack against **Fort McMurray International Airport** resulted in **7 days of business shut down** for administration employees, and took **6-8 weeks for system rebuilding** and full restoration of services
- + This tale has been talked about by many cyber security “experts” but they don’t know the real story. Or the real story a CEO needs to hear...
- + Over to RJ Steenstra, CEO of Fort McMurray International Airport
Every great war story starts with

“So, there I was in.....”



What ~~can you do~~ WILL YOU DO to LEVEL UP the Cyber “Boardroom Discussion”

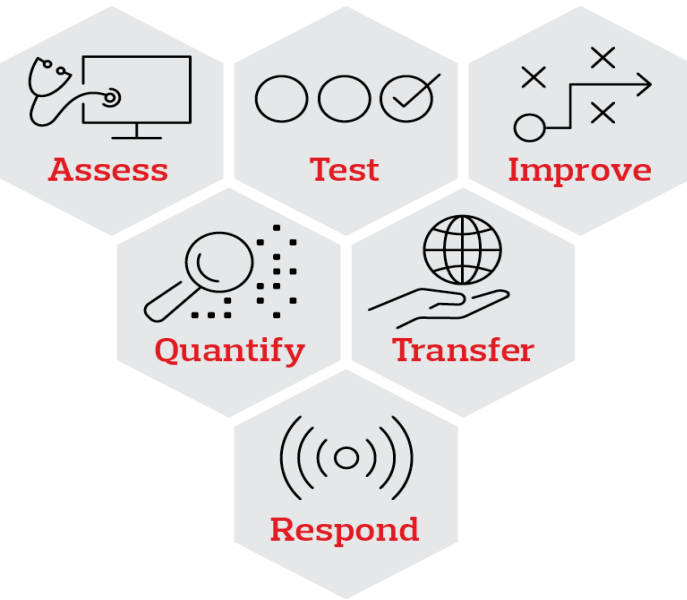
From the Desk of the CEO – “Cyber is not just Hackers and Breaches”

Human Resources

- Do we have the right auditing, electronic discovery, and investigations capabilities in place for the most common risks and case types?
 - Does our CULTURE make us vulnerable for social engineering?
 - How will we detect and investigate an INSIDER THREAT?
 - What benefits or protections to our teams, executives or partners can make us more secure at work and at home?
-
- Concessions
 - Do we know the security level and issues around our vendors?
 - How are their networks, data and other things hooked to airport operations?
 - Are we informed of problems, breaches or data thefts by employees?
 - How will we RESPOND together in a real incident? (Table Tops)

What Can Airport “Non-Security” Executives Do Today? FRAMEWORKS

Identify and protect your critical assets and balance sheet by aligning your cyber enterprise risk management strategy with your corporate culture and risk tolerance.



Finance officers can ask for the framework your team is using and then ask for a “business level” explanation of budget allocation in cyber discussions

Discussion Example ONLY – not recommended allocation

- 30% to security architecture development and deployment (protect)
- 10% to Assess and Test
- 10% to Improve
- 15% to Detect
- 10% to Quantify and Mitigation (Continuity Plans, COOP, Backups, etc.)
- 20% to Respond
- 5% to Training, Awareness and other areas

You improve, they re-target – budgeting for that?

- + Criminals always prefer to move from hard targets to softer ones.
 - Vendors, smaller organizations, easy entry points into the network.
- + Small and Medium Airport Cyber Collaboration?
- + Sharing threat intelligence and best technologies?
- + If any IT device is older than your children, its out of date.
- + If it is older than the AIRFRAMES landing at your airport, that is worse.

No matter who you use, this is a good list for a CEO to think about...



Seek

We help you understand and quantify your risk.



Shield

We know how to protect your organization and its critical assets.



Solve

We search for the truth and help you recover quickly.

- Assessments
 - > Security Risk Assessment
 - > CyQu
 - > Cyber Impact Analysis: Financial Quantification
 - > Incident Response Readiness Assessment
 - > Compromise Assessment
 - > Security Architecture Assessment
 - > Privacy Compliance Assessment
 - > Insider Risk Assessment
 - > Executive Vulnerability Assessment
- Testing
 - > Red Team & Social Engineering Testing
 - > Application & Mobile Security Testing
 - > Network & Cloud Penetration Testing
 - > Cloud & Host Configuration Review
 - > Automotive & IoT Security Testing
 - > Source Code Security Review
- Due Diligence & Background Investigations
- Cyber Insurance
- Cyber Risk Financing
- Incident Response Planning & Playbook Development
- Cyber Threat Simulation/Tabletop
- Security Architecture & Design
- Security Policies & Standards Development
- Security Strategy Development
- Security Controls Optimization
- Third Party Cyber Risk Management
- Insider Risk Program Development
- M&A Cyber Due Diligence
- Secure Software Development Lifecycle
- SOC Optimization
- CISO Advisory
- Board Advisory
- Fraud Prevention
- Stroz Friedberg Incident Response
- Stroz Friedberg Digital Forensics
- eDiscovery
- Expert Witness Testimony
- Incident Response Retainer
- Complex Cyber Loss Preparation
- Claims Advocacy
- Fraud & Financial Loss Investigations
- Workplace Misconduct Investigations

Why Us?

- **Technical Acumen**
- **Comprehensive Risk Management**
- **Tailored Solutions**
- **Data & Analytics**

Call +1 202 421 6386

Bryan.Hurd@aon.com

Airports (every division) lets the world move - every day.



- + The protection of the Mission is you!
- + Be engaged, work together and be involved.
- + Stopping international crimes against our countries, companies and even our families.

One team, one mission.

Bryan.Hurd@aon.com

<https://www.linkedin.com/in/bryanhurd>





BONUS Slides for Discussion

The 8 Strategic Risks Facing ALL OF US



1 Technology

Embracing Digital Transformation Creates New and Unanticipated Risks



2 Supply Chain

Supply chain security wake-up calls grow more insistent



3 IoT

IoT is everywhere, and it is creating more risks than companies realize



4 Business Operations

Technology for operational efficiencies can lead to security deficiencies that disrupt organizations



5 Employees

Excess privileges and shadow IT increase employee risk



6 Mergers & Acquisitions

Vulnerabilities from deal targets increases as dramatically as M&A value



7 Regulatory

Managing the intersection of cyber security policy and enforcement



8 Board of Directors

Directors and Officers face growing personal liability relative to cyber security oversight

Cyber Attacks on Critical Infrastructure

Telecommunications



SURFACE WEB

Google
Bing Wikipedia

DEEP WEB

Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.

Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information

Multilingual Databases
Financial Records
Government Resources
Competitor Websites
Organization-specific Repositories

Social Media

(DARK WEB)

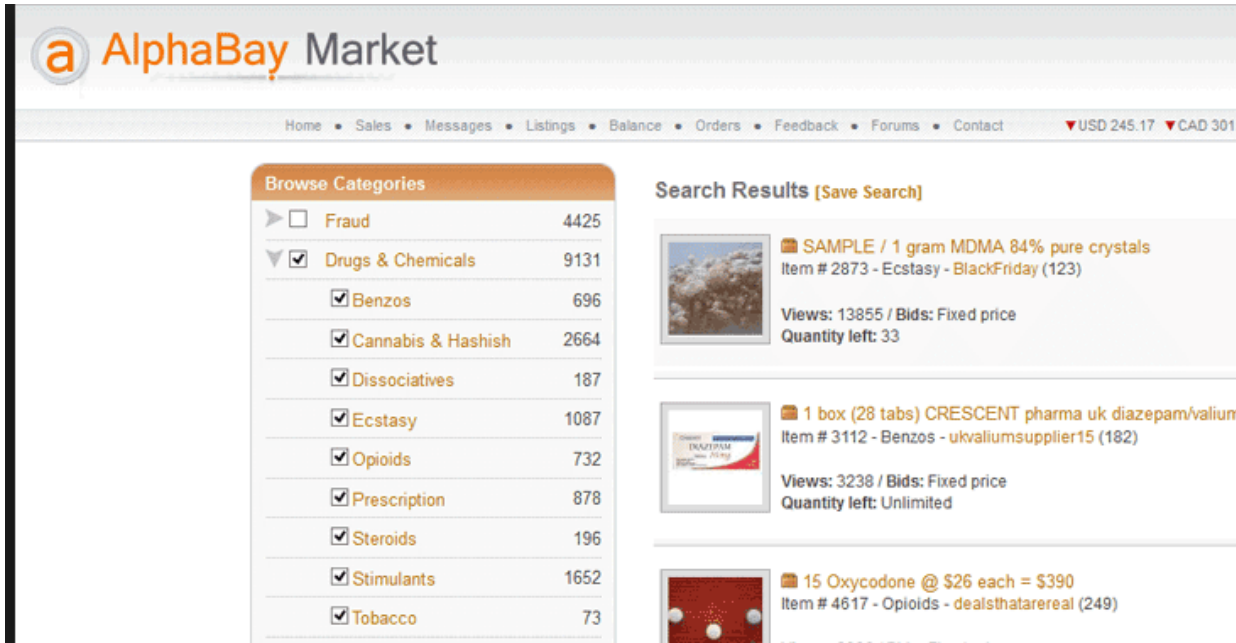
A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. Deep Web Technologies has zero involvement with the Dark Web.

Illegal Information
TOR-Encrypted sites

Political Protests




Drug Trafficking sites
Private Communications

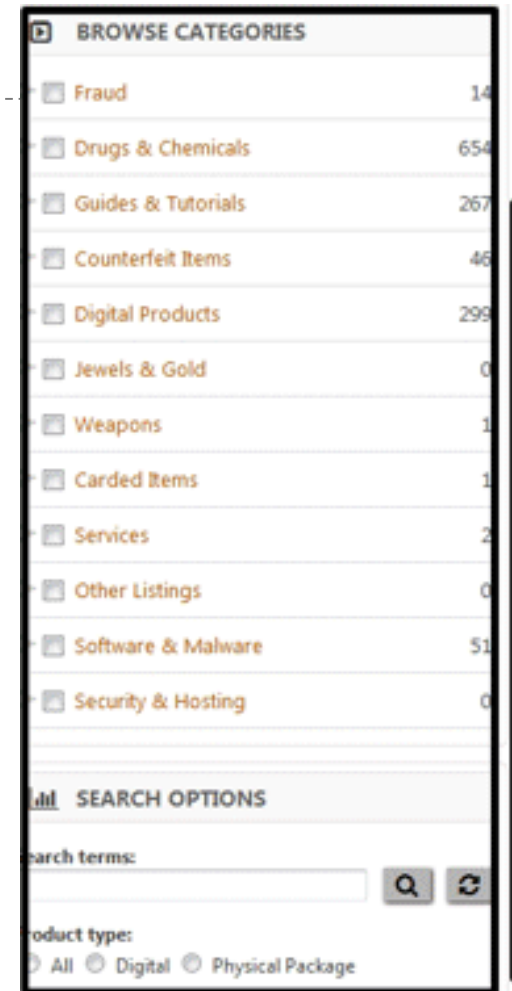
The DARK WEB looks really familiar.....and easy.



The screenshot shows the AlphaBay Market homepage. At the top left is the logo 'AlphaBay Market'. Below it is a navigation bar with links: Home, Sales, Messages, Listings, Balance, Orders, Feedback, Forums, Contact. On the right of the navigation bar are currency indicators: USD 245.17 and CAD 301.5. The main content area is divided into two columns. The left column is titled 'Browse Categories' and lists various categories with their respective item counts. The right column is titled 'Search Results [Save Search]' and displays three search results, each with a thumbnail image, a title, item number, and details like views and quantity left.

Browse Categories	
<input type="checkbox"/> Fraud	4425
<input checked="" type="checkbox"/> Drugs & Chemicals	9131
<input checked="" type="checkbox"/> Benzos	696
<input checked="" type="checkbox"/> Cannabis & Hashish	2664
<input checked="" type="checkbox"/> Dissociatives	187
<input checked="" type="checkbox"/> Ecstasy	1087
<input checked="" type="checkbox"/> Opioids	732
<input checked="" type="checkbox"/> Prescription	878
<input checked="" type="checkbox"/> Steroids	196
<input checked="" type="checkbox"/> Stimulants	1652
<input checked="" type="checkbox"/> Tobacco	73

Search Results [Save Search]	
	SAMPLE / 1 gram MDMA 84% pure crystals Item # 2873 - Ecstasy - BlackFriday (123) Views: 13855 / Bids: Fixed price Quantity left: 33
	1 box (28 tabs) CRESCENT pharma uk diazepam/valium Item # 3112 - Benzos - ukvaliumsupplier15 (182) Views: 3238 / Bids: Fixed price Quantity left: Unlimited
	15 Oxycodone @ \$26 each = \$390 Item # 4617 - Opioids - dealsthatarereal (249)



The screenshot shows the 'BROWSE CATEGORIES' section of the AlphaBay Market. It is a vertical list of categories with their respective item counts. Below the list is a 'SEARCH OPTIONS' section with a search terms input field and a 'product type' section with radio buttons for 'All', 'Digital', and 'Physical Package'.

BROWSE CATEGORIES	
<input type="checkbox"/> Fraud	14
<input type="checkbox"/> Drugs & Chemicals	654
<input type="checkbox"/> Guides & Tutorials	267
<input type="checkbox"/> Counterfeit Items	46
<input type="checkbox"/> Digital Products	299
<input type="checkbox"/> Jewels & Gold	0
<input type="checkbox"/> Weapons	1
<input type="checkbox"/> Carded Items	1
<input type="checkbox"/> Services	2
<input type="checkbox"/> Other Listings	0
<input type="checkbox"/> Software & Malware	51
<input type="checkbox"/> Security & Hosting	0

SEARCH OPTIONS

Search terms:

Product type: All Digital Physical Package

Click, Buy and BE EVIL

Botnets & Malware Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...

All your files have been encrypted

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

Stampado Ransomware - You always wanted a Ransomware but never wanted to pay hundreds of dollars for it? - This list is for you! Stampado is a cheap and easy to manage ransomware, developed by me and my team. It is sold by **The_Ramraker** - 2 sold since Jul 12, 2016

Vendor Level 1 Trust Level 5

Product class	Features	Origin country	Features
Digital goods		Worldwide	

v2.onion/listing/TMRvWlcqQF

GozNym 2.0 Banking Botnet

1500.00 USD

Second version of GozNym botnet. Installation on your bulletproof servers (1x Linux server for main & panel, 1x Windows server for HVNC \ Socks \ Backconnect). Or you can rent servers from me. PM me for full description.



Rent \ full license \ rental with support & crypt included options are available. Hit me up in Jabber.

First week of support is free. Some panel screenshots: <http://imgur.com/a/Qp6hb> PM for discussion.

onion 120%

[PACKAGE #3] - 1 MONTH C&C Dashboard (RaaS) - Price: 90 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- 1 Month C&C Dashboard access (to receive the AES keys from Clients)
- We take NO FEES from your Clients
- Features: Delayed Start, Mutex, Task Manager Disabler, UAC Bypass
- Platform: Windows (both x86 and x64)
- Support : Limited (initial setup only)
- Optional: additional Crypter adding 50 USD
- Optional: additional file types to encrypt for free (for all file types encrypted see FAQ)
- Optional: additional client banner in your language for free (already present en, ru, ge, fr, es, it, nl)

Intended to Test our Service

STROZ FRIEDBERG

an Aon company

© 2018 Stroz Friedberg. All rights reserved.

AON
Empower Results®

Airports (every division) lets the world move - every day.



- + The protection of the Mission is you!
- + Be engaged, work together and be involved.
- + Stopping international crimes against our countries, companies and even our families.

One team, one mission.

Bryan.Hurd@aon.com

<https://www.linkedin.com/in/bryanhurd>