Investment Recovery Association
2016 Conference & Tradeshow
Houston, TX

Cyber Security

Edward M. Stroz
Executive Chairman
STROZ FRIEDBERG

March 8, 2016

Our Purpose Today

- Introduction to the topic of “Cyber Security” and how to understand it
- Explain the dimensions of the problem and why it is so difficult to achieve cyber security
- Provide some important observations and trending questions we all face

Most “Cyber” Threats Use Software In Attack

“Malware” is harmful software (“code”)

- “Cyber” is a term to refer to computers and computer networks and how they communicate.
- Computers will carry out any instructions they are able to receive and process, and those instructions come in the form of software.
- Hackers are people who want to send unauthorized software (malware) to computers owned by other people.
- So, hackers usually want to get their malware on your computer. Think of their code as “poison” they want you to ingest, but they hide it in the food you would normally eat.

A real example of phishing scheme…

From: American Express <info@latinmarkets.org> Sent: Fri 8/8/2014 11:13 AM
To: Edward Stroz
Cc:
Subject: Security concern on your AmericanExpress Account

Dear Customer:

We are writing to you because we need to speak with you **regarding a security concern** on your account. Our records indicate that you recently used your American Express card on August 8, 2014.

For your security, new charges on the accounts listed above may be declined. If applicable, you should advise any Additional Card Member(s) on your account that their new charges may also be declined.

To secure your account , please click log on to : http://americanexpress.com

Your prompt response regarding this matter is appreciated.
Sincerely,
American Express Identity Protection Team

http://american-confess.com/americanexpress/
Click to follow link

Please do not reply to this e-mail. This **customer service e-mail** was sent to you by American Express. You may receive customer service e-mails even if you have unsubscribed from marketing e-mails from American Express.

Contact Customer Service | View our Privacy Statement | Opt Out

This email was sent to {_MAILTO_USERNAME}@{_MAILTO_DOMAIN}.

American Express Customer Service Department
P.O. Box 297817 | Ft. Lauderdale, FL 33329-7817

2014 American Express Company. All rights reserved.

SafeUnsubscribe

Trusted Email from Constant Contact
Try it FREE today.

This email was sent to estroz@strozfriedberg.com by info@latinmarkets.org |
Update Profile/Email Address | Rapid removal with SafeUnsubscribe™ | Privacy Policy.

American Express | 10 W. 37th Street 7th Fl. | New York | NY | 10018

From: Zaianna Ortiz [mailto:zaianna.ortiz@latinmarkets.org]
Sent: Friday, August 08, 2014 2:30 PM
To: Edward Stroz
Subject: Email Clarification Notice

LATIN MARKETS

Dear Colleagues,

Earlier this morning we experienced a breach to our third party email service provider account that resulted in many of you receiving a phishing email claiming to be from American Express with our email handle. American Express has confirmed that this is part of a large-scale Russian hacking, which you may have heard about earlier this week. American Express has advised our clients to forward any phishing emails to spouf@americanexpress.com to aide in their further investigations.

Our IT department recommends that you also delete these emails from your inbox and trash folders.

Please rest assured that under no circumstances will we ever share or sell your contact information with third parties.

I apologize for any inconvenience and encourage you to contact me directly with any questions or concerns.

Sincerely,

Zaianna Ortiz
Head of Marketing & Public Relations
Markets Group, US Markets/Latin Markets
+1 212-696-0878
Zaianna.ortiz@latinmarkets.org

LATIN MARKETS

The Malware Could be “Ransomware”

Malware Can Spy on You…

HOW CHINA'S SPIES CAN WATCH YOU AT YOUR DESK

60 Minutes reports on how the Chinese government steals trade secrets from American business people-and why CEOs in the U.S. keep it quiet

Dmitri Alperovitch and George Kurtz, founders of a computer security firm called CrowdStrike, demonstrate just how easy it is for Chinese spies to infiltrate American offices.

In some cases, they send a fake email to a U.S. worker that looks as if it comes from a colleague. If the worker clicks on the attachment, the Chinese hacker can not only steal documents, but also activate the computer's camera to watch the worker and listen in on conversations. The goal of such spying, the story explains, is for China to advance its own industries without putting in the research or funding required.

News Reports on the Malware

HOW CHINA'S SPIES CAN WATCH YOU AT YOUR DESK

60 Minutes reports on how the Chinese government steals trade secrets from American business people-and why CEOs in the U.S. keep it quiet

"This is different. This is taking our technology that our businessmen have spent money, energy, years developing, just taking it for themselves."

Can automobiles be hacked?

New high-end cars are among the most sophisticated machines on the planet, containing 100 million or more lines of code. Compare that with about 60 million lines of code in all of Facebook or 50 million in the Large Hadron Collider.

The New York Times

BUSINESS DAY

Complex Car Software Becomes the Weak Spot Under the Hood

By DAVID GELLES, HIROKO TABUCHI and MATTHEW DOLAN SEPT. 26, 2015

Lloyd Miller

Shwetak N. Patel looked over the 2013 Mercedes C300 and saw not a sporty all-wheel-drive sedan, but a bundle of technology.

How do we build trust from untrustworthy parts?

Vehicle control system depends on system components manufactured by different vendors

- Each vendor contributing parts to a car uses their own software and hardware
- Manufacturers like to develop components that will work for different kinds of vehicles (cheaper) which can spread the vulnerabilities across them
- The complexity of components like sensors, actuators, wireless communication, multicore processors are steadily increasing. Complex systems are harder to secure.

Are we engineering security into our devices?

Trusting Systems You Didn’t Build To Work Together Properly

- Development of control system may be independent of system implementation
- Challenge of integrating various subsystems while keeping them functional
- Research missing on understanding interactions between vehicle control systems and other subsystems:
    - Engine, transmission, steering, wheel, brake, suspension

Trains, Planes, Automobiles and…..

…Seagoing Vessels Are At Risk Too

- A recent demonstration by a UT Austin team showed how a potential adversary could remotely take control of a vessel by manipulating its GPS.
- The yacht “White Rose of Drachs” was successfully spoofed while sailing on the Mediterranean.
- The team’s counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship’s navigation system.
- “The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line.”

Here is the press story…

The White Rose of Drachs was coerced onto a parallel course as it travelled from Monaco to Rhodes

The Telegraph

By Sophie Curtis
8:17AM BST 31 Jul 2013

HOME » TECHNOLOGY » TECHNOLOGY NEWS

Researchers commandeer £50m superyacht with GPS-spoofing

Researchers at the University of Texas have succeeded in hijacking a 213-foot yacht as it sailed from Monaco to Rhodes on the Mediterranean Sea, by overriding its GPS signals.

The team, led by assistant professor Todd Humphreys from UT Austin's department of aerospace engineering and engineering mechanics, took a GPS "spoofing" device the size of a briefcase aboard the *White Rose of Drachs*, as it passed 30 miles off the coast of Italy.

From the upper deck, they were able to broadcast fake GPS signals from their spoofing device toward the ship's two GPS antennas, which slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system.

Unlike GPS signal blocking or jamming, spoofing triggers no alarms on the ship's navigation equipment, according to Humphreys. To the ship's GPS devices, the team's false signals were indistinguishable from authentic signals, allowing the spoofing attack to happen covertly.

Source: UT Austin "Know"

Maritime risks are not limited to vessels

Not Just Ships In The Water…

- Vulnerabilities extend to the entire maritime transportation system.
- Hackers recently shut down a floating oil rig by tilting it. (Reuters 4/23/14)
- Another rig was so riddled with computer malware that it took 19 days to make it seaworthy again. (Reuters 4/23/14)

Certain systems are especially important

Some of our nation's most important critical infrastructure is increasingly controlled by computer networks

- Power systems ("smart grid")
- Transportation systems ("smart transportation")
- Water supply systems
- Air traffic control
- Building control systems ("smart buildings")
- This infrastructure is potentially vulnerable to failures of computer systems or deliberate cyber attacks

The federal government has identified…

16 Critical Infrastructure Sectors


Chemical


Commercial Facilities


Communications


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy


Financial Services


Food & Agriculture

Government Facilities


Healthcare & Public Health

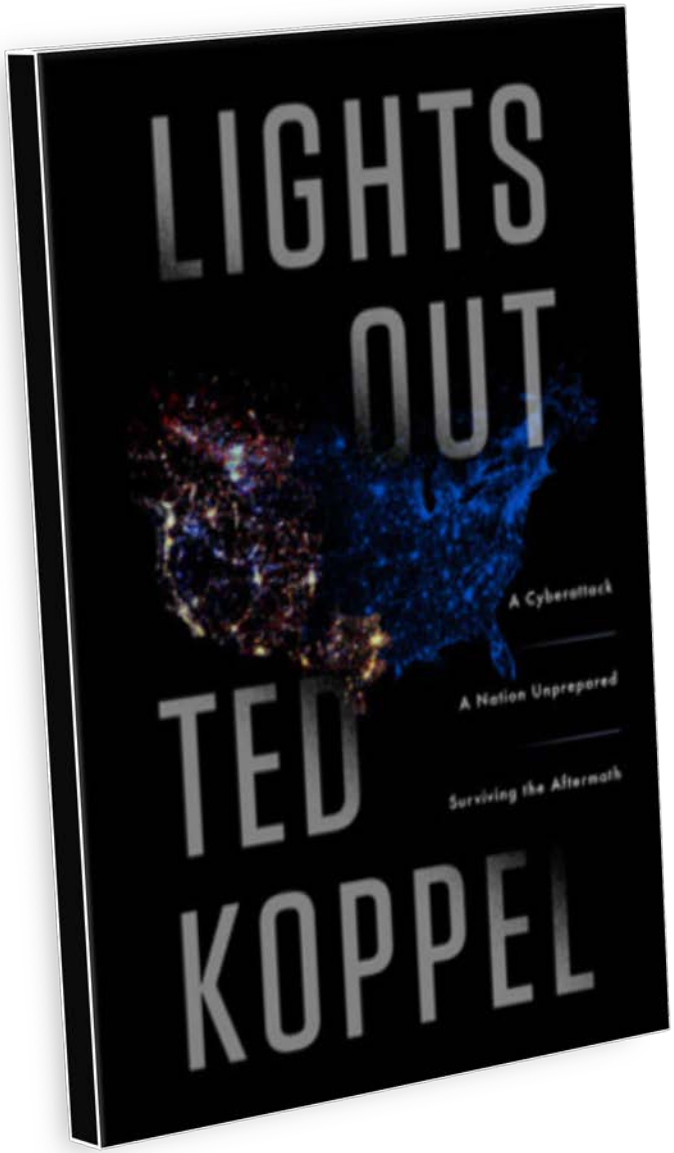

Information Technology


Nuclear Reactors, Materials, & Waste


Transportation Systems


Water & Wastewater Systems

We are improving our understanding of the risks…



Critical Infrastructures Use SCADA Systems

WIKIPEDIA
The Free Encyclopedia

SCADA

From Wikipedia, the free encyclopedia

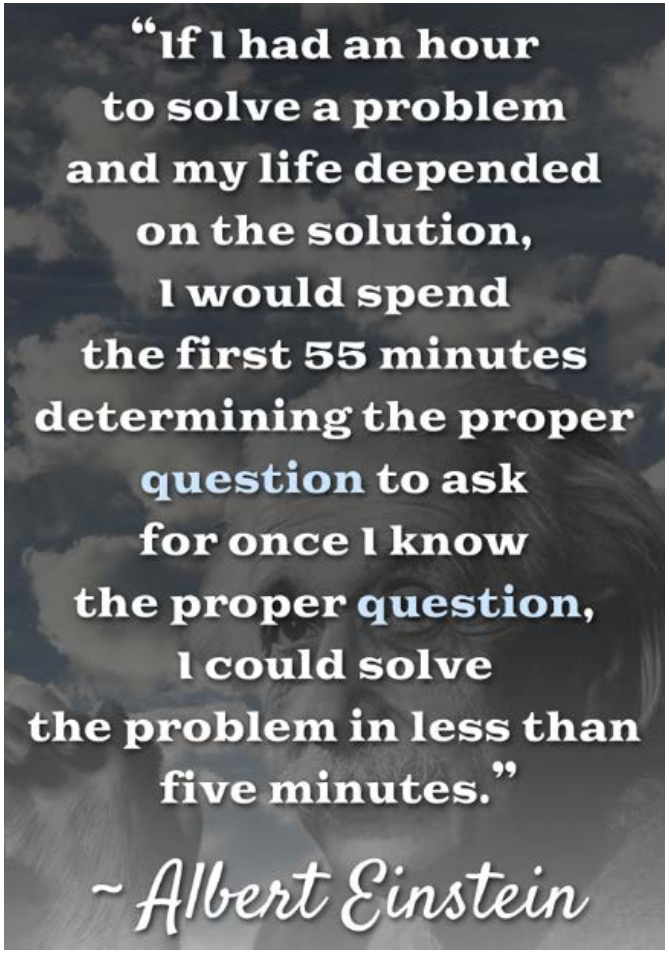
SCADA (**supervisory control and data acquisition**) is a system for remote monitoring and control that operates with coded signals over communication channels (using typically one communication channel per remote station). The control system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions.[1] It is a type of industrial control system (ICS). Industrial control systems are computer-based systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large-scale processes that can include multiple sites, and large distances.[2] These processes include industrial, infrastructure, and facility-based processes, as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access, and energy consumption.

What are the right questions to ask?

A More Beautiful Question

The power of inquiry to spark breakthrough ideas



Trending questions everyone asks:

- How do you build a trustworthy platform from untrusted components?

- With three billion people on line today using a trillion devices, how do we insure the integrity of our information in an open society?

- “National security” is strategic and driven from the top, but “homeland security” is decentralized and works largely from the ground up. How do we ensure they are complementing each other?

- Is our organization paying enough respect to basic computer “hygiene” given that it is one of the most important aspects of security. It's where 80% or more problems arise.

- Secrecy and privacy are essential, but they do not scale.

Boards of Directors are asking:

- How do we know who is logging into our network, and from where?
- How do we track what digital information is leaving our organization and where it is going? Do we have an effective data loss prevention program?
- Which cyber threats and vulnerabilities pose the greatest risk to the organization's business and reputation? What are the key assets to be protected? What is our strategy to address identified weaknesses?
- What systems are in place to protect information transferred through mobile technologies? Is there a culture of responsibility with regard to each employee's responsibilities in using mobile devices?

Audit/Risk Committees are asking:

- Is management focused on making cyber-risk part of everyone's job, and not just IT's?
- Do we have the right gauges and metrics to measure the success of our cyberthreat management program?
- Are we planning to map our policies to the NIST Framework, or something similar? If we are already following an industry-recognized standard, how much effort would it take to map the steps we have already taken to another framework?
- What are our training programs to educate our workforce about cyber risks and responsibilities?

Your Questions?