



The ONE Key Cyber Security Element is Your Human Factor

by

Dane A. Deutsch

CEO/DCS Netlink

www.dcsnetlink.com

ddeutsch@dcsnetlink.com

877-327-6385

A Service Disabled Veteran Owned Small Business Company

© 2018 All Rights Reserved – DCS Netlink

Did You Know?



internet live stats

live

1 second

watch

trends & more

Get our Counters!



3,834,931,348

Internet Users in the world



1,326,009,599

Total number of Websites



107,164,596,619

Emails sent [today](#)



2,517,055,847

Google searches [today](#)



2,366,998

Blog posts written [today](#)



306,449,784

Tweets sent [today](#)

Develop Processes & Procedures to Minimize the Human Factor



Today's Briefing:

- Introduction - Dane & Bobby Blackhat
- Examples of the REAL Threat
- The Key to Security Processes & Procedures
- Increase Cyber Awareness
- Create a Budget
- Identify Weak Links
- Identify Security Breaches
- What to do when breached or compromised

My Background



- Introduction to Bobby Blackhat
- Dane is a US Air Force Retired Officer
- Last USAF Active Duty Assignment
 - IT Chief of Maintenance for the country of Turkey
 - All wireless in 1980's; first email server; and more
 - Technology in Turkey was more modern than US Today!
- Last 27 years building our IT business
 - DCS Netlink - focused on leading IT with security
 - DCS=Dynamic Cloud Solutions
 - FBI Secured Infragard Members
- www.dcsnetlink.com & www.intersecwi.com

Ex#1- Cate Machine & Weld



Small Wisconsin Manufacturing Company taken over by Chinese!

And like many small businesses, they have a dusty old computer humming away in the back office. On this one, however, an unusual spy-versus-spy battle is playing out: The machine has been taken over by Chinese hackers.

The hackers use it to plan and stage attacks.

<http://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html>

Ex #2 - Closer to Home



- **Barron School District - W-2 Story**
- **145 Businesses had W-2s Phished before 2017**
- **Schools & Businesses have NO budget for Risk Assessment**
- **Equifax Breach was really BAD for all of us!**
- **Things have changed, but WE have NOT!**

Ex #3 - Social Engineering Hacker



The Enemy may actually be.....



US!

Tiger Team



The Enemy may actually be.....



US!

**We think the problem is always with someone else!
We think if it hasn't happened, it most likely won't happen!**

Trust builds Relationships & is the Key to Security!

**Your future is only as secure as you make the choice to BE and
who you Choose to be connected with!**

Make sure you are partnered with a company that leads with Character 1st!

Verify 1st and Trust 2nd!

Introduction to NIST

Greg Rattray

Managing Director, JP Morgan Chase



Processes & Procedures



- NIST Framework Introduction: <https://www.nist.gov/cyberframework>
- *“What does not get measured does NOT get done”*

NIST Search NIST **≡ NIST MENU**

CYBERSECURITY FRAMEWORK

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure

- Cybersecurity Framework (PDF)**
- Cybersecurity Framework (Excel)**
- Draft Version 1.1**
- Industry Resources**
- Frequently Asked Questions**
- Events and Presentations**

Latest Updates

- RFC comments received on [Draft 2](#) of Framework Version 1.1 and the [Roadmap](#) are now being reviewed. All responses will be published publicly in the coming weeks. NIST appreciates your feedback and as always, any additional comments can be directed to cyberframework@nist.gov.
- Two December 2017 [webcasts](#) about Framework basics and the proposed updates to Framework and Roadmap are now available for playback.
- A mapping of the Framework Core to NIST SP 800-171 Revision 1 has recently been published. This can be found in Appendix D of the [publication](#).
- A blog entry on protecting critical infrastructure has been posted. [A Framework for Protecting our Critical Infrastructure](#).

Cyber Landscape Today



- **Dangerous! What if I told you...?**
 - First time in history that the US Government & military can't protect us as citizens
 - 4 Star Generals still can't stand up a Cyber Command
 - Past NSA person says, "Chinese are in every one of our systems....it is only a matter of time."
 - Media has reported government and business being hacked at one time or another (i.e.- US Army, US Senate)
 - Cyber threats are increasing in quantity and severity
- **Houdini Concept - If built by mankind, then it can be broken into by mankind.**
- **HUMAN FACTOR is the Weakest Link!**

8 State Manufacturer Story



Hackers siphoned money from their accounts 3 times before being stopped!

They had no idea how the “bad guys” were getting into their network, nor how the money was being siphoned.

Yet, the CEO and Owner had never put any processes or systems in place to identify or find the bad guys.

TOP HUMAN FACTOR THREATS



- **NO Budget - no money to prepare and stay prepared!**
- **NO Security processes/procedures - IT guy is enough!**
- **NO Security Awareness Training Program**
- **NO way to measure and improve the “weak links”**
- **NO alerting mechanisms in place to ID a breach**
- **NO idea of who to call? Coachable?**

NIST Cyber Security Framework



7 Keys to strengthen Human Factor



1. **Beliefs**: Start w/Culture and Character from the Leadership!
1. **USE NIST Framework - Map of what to do and steps to take!**
1. **DO regular Risk Assessments!**
1. **Passwords - Use an Enterprise PW Manager!**
1. **Social Engineering** - Educate and Measure - continuously!
1. **Monitor the Dark Web** -get alerts on your domain!
1. **Get Managed Services**
1. **Firewall Logging** Turned ON!

CALL TO ACTION!



1. **Partner/Team** with a reputable cyber security Company!
2. Make sure you have a **budget!**
3. Use **NIST framework** to outline your needs
4. **FREE Dark Web Scan** - contact me after seminar.
5. **Phishing Test & Measurement** used consistently!
6. **Risk Assessment** is a 2nd great step!
7. **Managed Services** is critical for Realtime Monitoring!
8. Create a new **Mindset** that Cyber Security is an everyday....

BE Coachable and a TEAM!

Develop Processes & Procedures to Minimize the Human Factor



Today's Briefing:

- Introduction - Dane & Bobby Blackhat
- Examples of the REAL Threat
- Processes & Procedures
- Increase Cyber Awareness
- Identify Weak Links
- Identify Security Breaches
- What to do when breached or compromised

MISSION



*Identify the enemy on the Internet &
how to protect against those threats*

“US - You and I”

WE are The Human Factor

WE are the GREATEST THREAT!



The ONE Key Cyber Security Element is Your Human Factor

by

Dane A. Deutsch

CEO/DCS Netlink

www.dcsnetlink.com

ddeutsch@dcsnetlink.com

877-327-6385

A Service Disabled Veteran Owned Small Business Company

© 2018 All Rights Reserved – DCS Netlink