INTERNET SECURITY ALLIANCE

For information about membership opportunities, please contact:

Larry Clinton

President & CEO

lclinton@isalliance.org

(703) 907-7028

For more information about the Internet Security Alliance, please visit www.isalliance.org

Digitalization Changes Everything

- The way our brains function
- The way we define ourselves
- Our notions of what privacy is
- Our assumptions about how to conduct national defense
- Our assumptions about economics
- Our assumptions about security

How confident are you (should you be)?

- 80% of CEOs are "very confident" – but successful compromises up 66%
- Losses will jump from $500 billion to $2 trillion by 2018 – up 2x as much as security spending
- 71% of attacks are on firms w/less than $2 billion
- CEOs still prioritize keeping the bad guys out
- CEOs agree they need better ways to measure success

Benchmarking DoD --- Things are really bad

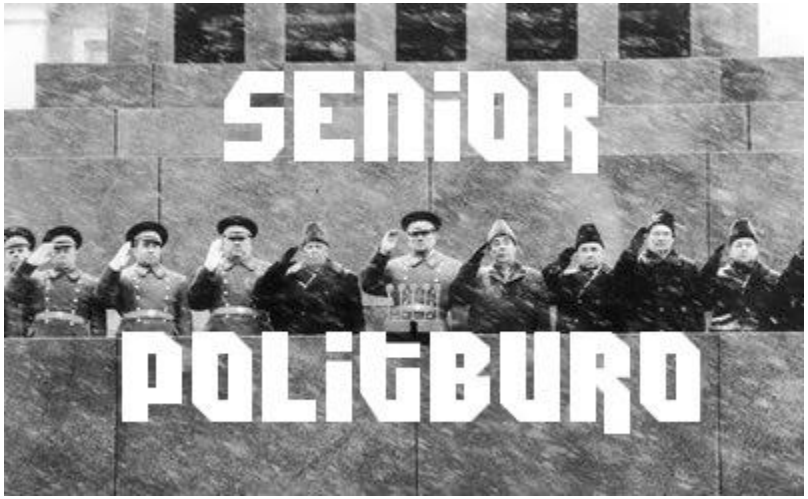
The military's computer networks can be compromised by **low to middling skilled** attacks. Military systems do not have a sufficiently robust security posture to repel sustained attacks. The development of advanced cyber techniques makes it likely that a determined adversary can acquire a foothold **in most DOD systems** and be in a position to degrade DOD missions **when and if they choose**." Pentagon Annual Report Jan 2015.

Things are going to get worse …

- The attackers are getting much better
- All the economic incentives favor the attackers
- The system is getting technologically weaker

INTERNET SECURITY ALLIANCE

Kremlinology



INTERNET SECURITY ALLIANCE

Trumpology

Lt. Gen. Michael Flynn
National Security Advisor

General Keith Kellogg
National Security Council

Steven Bannon

Donald McGahn
General Counsel

Gen. James Mattis
Sec of Dep. of Defense

Mike Pence
Vice President

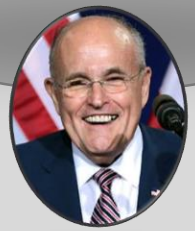
President Donald Trump

Tom Bossert
Homeland
Security Advisor

Gen. John Kelly (USMC – Ret.)
Sec of Dep. of Homeland Security

Josh Steinman

Karen Evans



Rudy Guiliani
Former Mayor of NYC

Governor Rick Perry
Sec. of Dep. of Energy

Adm. Mike Rogers
Director of National
Intelligence

Cybersecurity in the Power Utilities Sector

1. Enhance information sharing between utilities and the federal government.
2. Reforming the clearance-attainment process for private-sector executives.
3. Ensure DoE remains the primary liaison between utilities and the federal government.
4. Catalyze and accelerate the development of the private cybersecurity insurance market.
5. Promote innovation through government grants.

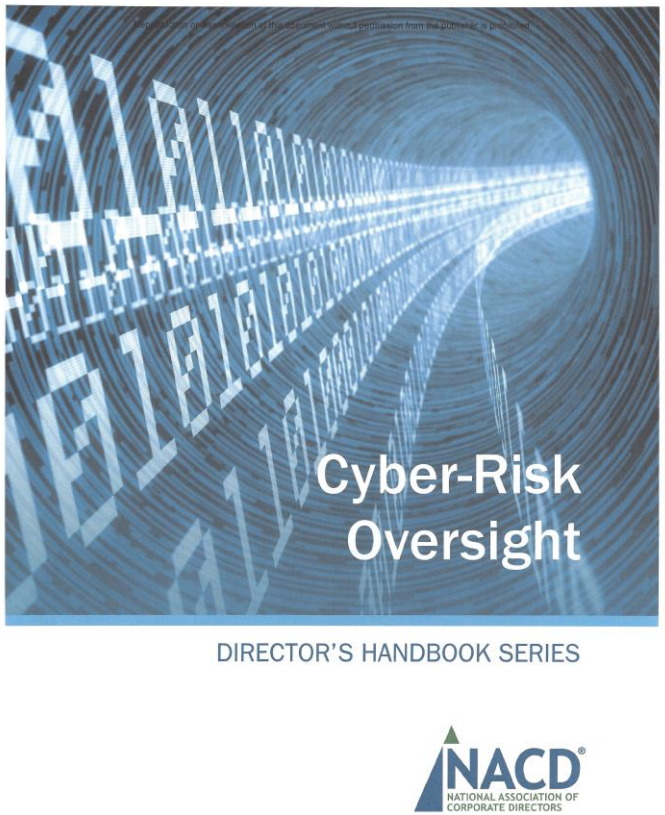
Cybersecurity in the Power Utilities Sector

6. Increase cybersecurity focus of state-level regulators and legislatures.
7. Encourage public-private collaboration to manage vendor risks.

Necessary Steps for Small and Medium-Sized Organizations

1. Have an information security policy.
2. Patch your systems and applications, and probably do it automatically.
3. Require multi-factor authentication.
4. Restrict employee's ability to surf the web on company computers.
5. Train employees on cybersecurity practices.
6. Scan and filter email and web traffic.
7. Set up logging and store the data for the long-term

ISA/NACD Cyber-Risk Oversight Handbook



Copies of the ISA/NACD Cyber-Risk Oversight Handbook can be obtained at:
http://www.isalliance.org/cyber-risk-handbook

Corporate Boards are getting involved

- Guidelines from the NACD advise that Boards should view cyber-risks from an enterprise- wide standpoint and understand the potential legal impacts. They should discuss cybersecurity risks and preparedness with management, and consider cyber threats in the context of the organization's overall tolerance for risk. -- PWC 2016 Global Information Security Survey

Boards are taking action

- Boards appear to be listening to this advice. This year we saw a double-digit uptick in Board participation in most aspects of information security. Deepening Board involvement has improved cybersecurity practices in numerous ways. As more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending. --- PWC 2016 Global Information Security Survey

Actual Cyber Security Improvements

- Notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals. Perhaps more than anything, Board participation opened the lines of communication between the cybersecurity function and top executives and directors -- PWC 2016 Global Information Security Survey

ISA Comments to CAQ

1. These proposed engagements are assessments, not audits.
2. Measuring cyber assessments should use a maturity model.
3. Cybersecurity is not all about “IT”.
4. Assessment tools need to focus primarily on techniques with proven effectiveness and cost effectiveness.
5. The assessment tool needs to be a voluntary model – really voluntary.
6. We need to assure there will be adequate Talent Availability to perform the assessments.