FORENSECURE ‘19
INFORMATION ASSURANCE/CYBERSECURITY REQUIREMENTS FOR WORKING WITH THE US GOVERNMENT
Dr. David Anderson

- Dept. of Computer Information Systems, Triton College, River Grove, IL 60171
- davidanderson@triton.edu

Dr. Karl Reimers

- Tillman School of Business, University of Mount Olive, Mount Olive, NC 28365
- kreimers@umo.edu
Dr. Anderson is a retired U.S. Army officer, civilian system engineer (AllState, Raytheon), and educator in Information Technology (especially networks and security). He has published both books and papers on the topics.

Has been at Triton College since 2001 where he is currently Coordinator and Professor in the Computer Information Systems (CIS) Dept.

Has a doctorate degree in Information Technology as well as various Information Technology industry certifications (CompTIA, Cisco, CIW, Microsoft) and member of the FBI Infragard Chicago.

Linkedin: https://www.linkedin.com/in/drdanderson/
• There has been a phenomenal surge in the use of Information Technology.
• 7.2 billion digital devices as of Dec 2018.
• Average IT salary is $84,000
  Data-security analyst is $121,000
  IT security manager is $137,000
  (Depends on where you look)
• IT unemployment is under 2%
• Cybersecurity unemployment is under 0%
In the money: Metros that pay the most for information security specialists

*Annual salary adjusted for cost of living*

<table>
<thead>
<tr>
<th>Rank</th>
<th>Metro area</th>
<th>Adjusted</th>
<th>Unadjusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Charlotte, NC</td>
<td>$125,173</td>
<td>$117,533</td>
</tr>
<tr>
<td>2</td>
<td>Chicago, IL</td>
<td>$119,887</td>
<td>$125,668</td>
</tr>
<tr>
<td>3</td>
<td>San Francisco, CA</td>
<td>$116,073</td>
<td>$148,621</td>
</tr>
<tr>
<td>4</td>
<td>Austin, TX</td>
<td>$113,126</td>
<td>$125,668</td>
</tr>
<tr>
<td>5</td>
<td>Denver, CO</td>
<td>$112,206</td>
<td>$148,621</td>
</tr>
<tr>
<td>6</td>
<td>Philadelphia, PA</td>
<td>$110,943</td>
<td>$118,403</td>
</tr>
<tr>
<td>7</td>
<td>Boston, MA</td>
<td>$103,953</td>
<td>$115,890</td>
</tr>
<tr>
<td>8</td>
<td>Baltimore, MD</td>
<td>$103,944</td>
<td>$112,372</td>
</tr>
<tr>
<td>9</td>
<td>San Jose, CA</td>
<td>$97,344</td>
<td>$128,253</td>
</tr>
<tr>
<td>10</td>
<td>New York, NY</td>
<td>$98,159</td>
<td>$125,684</td>
</tr>
</tbody>
</table>
THE BAD

- Record number of security issues:
- Each year is a new “record year”
- New problems keep appearing
- Dark web – children’s personal data for sale
The Certified Financial Planner Board of Standards says nearly a third of lottery winners declare bankruptcy—meaning they were worse off than before they became rich.

Other studies show that lottery winners frequently become estranged from family and friends, and incur a greater incidence of depression, drug and alcohol abuse, divorce, and suicide than the average American.

So forget it. 😊
SIGNIFICANCE OF THE PROBLEM

- Data security incidents continue, including the largest distributed denial-of-service (DDoS) attack ever recorded at 1.7Tbps.
- In just one year, the initial costs attributable to cyberattacks increased 52% to $1.1 million ($2 trillion nationally).
- Two in five companies reported negative customer experiences and reputation loss following a successful attack.
- Ninety-three percent of respondents experienced a cyberattack in the past 12 months; only seven percent claimed not to have experienced an attack.
- Cyberattacks were a weekly occurrence for one-third of organizations.

SIGNIFICANCE OF THE PROBLEM

• We are seeing modes of attack on corporate networks shifting away from mass probing of large numbers of computers to social engineering thrusts targeted at particular individuals.
  - Malware, Phishing, DOS, Ransomware, Personal data.

• Hackers are using careless social media users to gain entry into network systems and work their way up to more senior people and parts of the network containing sensitive information.

• 50% of Industrial Control System Networks have faced cyberattacks

Source: ZDNet, Palmer, D., March 27, 2019
WHAT IS INDUSTRY SAYING?

What's in an internet minute? According to data from RiskIQ and threat researchers around the world, a lot of evil.

**2018 COST OF CYBER CRIME**

**TOTAL COST**
- $600 BILLION¹
- $1,138,888/minute
- $171,233/minute spend by business on information security²

Global, the cost of cybercrime on large business ranged from 11.7 MILLION/year³
- Ranging from $222/minute

**CYBERCRIME VICTIMS**
- 2.7 MILLION/day⁴
- 1,861/minute

**RANSOMWARE**
- costs to organizations
  - $8 BILLION/day⁵
  - $15,221/minute⁵
  - 1.5 organizations/minute fall victim to ransomware attacks⁶

**MALWARE**
- 1,274 new malware variants/minute⁷

**PHISHING EMAILS**
- 22.9 attacks/minute⁸

**RECORDS LEAKED**
- from publicly disclosed incidents
  - 2.9 BILLION/day⁹
  - 5,518/minute
WHAT ARE MEDIA SAYING?

Cybercrime groups continue to flourish on Facebook
April 2019

Russian Mega-Hacker Pleads Guilty in Largest U.S. Breach
Vladimir Drinkman Played a Lead Role in Massive Cyber-Attack

OM government data breach impacted 21.5 million
CNN July 10, 2015

Goodwill Vendor Describes Breach
18-Month Malware Attack Affected 3 Clients
By Jeffrey Roman, September 16, 2014. Follow Jeffrey @gen_sec

80 Million Potentially Impacted By Anthem Security Breach
February 5, 2015

UPS Reveals Data Breach
POS Malware Compromises 105,000 Transactions at 51 Stores
By Mathew J. Schwartz, August 21, 2014. Follow Mathew J. @eurinfosec

JPMorgan Employee Password Was Key in Hack Hitting 76 Million Homes
By Hugh Son, Oct 2, 2014 7:39 PM ET 605 Comments Email Print

Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data
Forbes March 17, 2015

Home Depot hack could lead to $3 billion in fake charges
By MITCH LIPKA MONEYWATCH. September 16, 2014, 8:06 AM

Sutter Health Incident Illustrates Email Risks
Marianne Kolbasuk McGee September 14, 2015
WHAT ARE TRACKING SITES SAYING?

- 300+ Million records (so far) in 2018
- Targets include all industries and geographies
- Healthcare shows a recent spike in breach activity
- Social engineering has replaced brute force hacking
- Victims include industry leaders with huge budgets

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
WHAT ARE OTHERS SAYING?

ISACA Study

- Non-malicious insiders are #2 threat actors behind hackers
- Phishing, malware, hacking and social engineering are top attack types
- Loss of mobile devices is next most common “attack type” (44%)
- Over 82% provide mobile devices and 91% report loss of mobile devices
- Almost 80% report their Board:
  - say they are concerned with security
  - only 40% practice good security

WHAT ARE OTHERS SAYING?
(continued)

PwC Global State Survey

- 91% or organizations have adopted risk-based security frameworks
- 91% use some form of advanced authentication
- Top issues are malware, provisioning, PII protection and end-user vulnerabilities
- Only 50% have a CISO
- Less than 50% have Board participation in security strategy
- Sources of compromise are current/former employees, followed by service providers – <90%

Source: http://www.pwc.com/gx/en/issues/cybersecurity/information-security-survey/download.html
Nation-states have the same problems large organizations do.
The threats to nation–states tend to be ignored.
Nation-states have special problems – elections, govt., etc.
Elections

- OTOH – there are thousand’s of state and local election entities – all distinct.
- OTOH – the 2000 presidential election between George W. Bush and Al Gore - was decided by just 537 votes in the state of Florida
When considering PC/Network protection for your house, apartment, or cardboard box under a bridge, the single most effective step is to...

A. Keep teenage males off of your PC’s and phones
B. Install all the antivirus software you can find
C. Bury your digital stuff in a hole in your back yard
D. Own nothing, Grasshopper 😊
When considering PC/Network protection for your house, apartment, or cardboard box under a bridge, the single most effective step is to...

A. Keep teenage males off of your PC’s and phones
B. Install all the antivirus software you can find
C. Bury your PC’s in a hole in your back yard
D. Own nothing, Grasshopper 😊

Nation-states can’t do any of the above 😞
SIGNIFICANCE OF THE PROBLEM
• Offense: Nation-states as well as larger organizations, are creating cybersecurity/hacking “units” for the express purpose of penetrating foreign organizations.

• Defense: Nation-states as well as larger organizations, are creating cybersecurity/hacking “units” for the express purpose of defending against foreign and domestic organizations.
SIGNIFICANCE OF THE PROBLEM

DISSECTING THE 2018 THREAT LANDSCAPE


Figure 3. Regional trends in changing motivations for cyberattacks.
Every nation-state has its own focus:

- Russia – sow discord – weaken unity ("Russia master of the viral tweet") (Chicago Trib “tweet of the month Dec 2018”)
- China – infrastructure penetration
- North Korea – financial gain
- U.S. – national security (Stuxnet worm), foreign elections, NSA
The theory is great, but the reality is flawed.

U.S. and Russia – agreement, but ...

U.S. and China – agreement, but ...
Secret Service agents arrested a Chinese woman at Mar-a-Lago carrying a thumb drive containing malicious software (WP, Apr 2, 2019)

U.S. and NATO – agreement, but ...

We can assume other countries have the same problem ...
America Goes on the Cyberoffensive

U.S. government hackers will now have greater latitude to deter and answer attacks.
FBI, Retooling Once Again, Sets Sights on Expanding Cyber Threats

Push comes as federal investigators grapple with attacks sponsored by foreign adversaries
New York Launches a Cybercrime Brigade
A new citywide initiative aims to coordinate digital law-enforcement efforts.

By Cy Vance Jr. and James P. O'Neill
April 1, 2019 7:08 p.m. ET

A Department of Justice news conference about computer hacking in Washington, Nov. 28, 2019. PHOTO: JOSE LUIS MAGANA/ASSOCIATED PRESS

In a little more than a month last year, cybercriminals temporarily debilitated Atlanta’s computer systems, disrupted Baltimore’s 911 emergency system, and forced Colorado’s Department of Transportation offline. Atlanta’s cyberattack alone cost taxpayers an
More than half (54%) of companies plan on increasing IT security spending in 2019.

30% of companies aim to increase spending by 10-20%.

One in three companies said they don't feel ready to combat a cybersecurity threat.
WHERE THE MONEY IS

Top Industry, Based on Five-Year CAGR (2017–2022) (Value, Constant Annual)

<table>
<thead>
<tr>
<th>Industry</th>
<th>CAGR (5 Years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal/Central Government</td>
<td>+8.0%</td>
</tr>
<tr>
<td>Discrete Manufacturing</td>
<td>+7.8%</td>
</tr>
<tr>
<td>Utilities</td>
<td>+7.7%</td>
</tr>
<tr>
<td>State/Local Government</td>
<td>+7.6%</td>
</tr>
<tr>
<td>Banking</td>
<td>+7.6%</td>
</tr>
<tr>
<td>Others</td>
<td>+6.7%</td>
</tr>
</tbody>
</table>


Source: IDC
WHERE THE MONEY IS

Cybersecurity deployment in transition

- Source: Canalys
Since the 1990s, Information Technology (IT) certifications have increased in number and influence throughout the information technology career field and subfields.

McKillip and others have established and then reaffirmed the validity of technical certifications.
WHY CERTIFICATIONS?

- Many academic programs such as the accounting, engineering, law, medical, and teacher education disciplines, focus instruction on preparing students for licensing exams.

- Example: Preparation for the Certified Public Accountant (CPA), Professional Engineer (PE) or other state licensing exams is integral to the programs in most institutions that teach the subject.
The field of commercial and government information technology has long considered certification a necessary qualification for employment. Employers have often required their employees to have pertinent IT certifications when hired or to obtain them within a specified period after hire.
A new credentialing system grew out of the demand for certification procedures.

In 1989, the Certified NetWare Engineer (CNE) program developed by Novell Education became the first IT industry credentialing system to gain widespread support.

A decade later, more than 1.7 million credentials were awarded by a burgeoning system of competency-based training and certification.
THERE ARE A LOT OF IT SECURITY CERTIFICATIONS – OVER 100

<table>
<thead>
<tr>
<th>Credential abbreviation</th>
<th>Certification Title</th>
<th>Issuing Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISSP</td>
<td>Certified Information Systems Security Professional</td>
<td></td>
</tr>
<tr>
<td>CISSP-ISSAP</td>
<td>Information Systems Security Architecture Professional</td>
<td></td>
</tr>
<tr>
<td>CISSP-ISSEP</td>
<td>Information Systems Security Engineering Professional</td>
<td></td>
</tr>
<tr>
<td>CISSP-ISSMP</td>
<td>Information Systems Security Management Professional</td>
<td></td>
</tr>
<tr>
<td>SSCP</td>
<td>Systems Security Certified Practitioner</td>
<td>(ISC)²</td>
</tr>
<tr>
<td>CCSP</td>
<td>Certified Cloud Security Professional</td>
<td></td>
</tr>
<tr>
<td>CAP</td>
<td>Certified Authorization Professional</td>
<td></td>
</tr>
<tr>
<td>CSSLP</td>
<td>Certified Secure Software Lifecycle Professional</td>
<td></td>
</tr>
<tr>
<td>HCISPP</td>
<td>HealthCare Information Security and Privacy Practitioner</td>
<td></td>
</tr>
<tr>
<td>Security+</td>
<td>CompTIA Security+</td>
<td></td>
</tr>
<tr>
<td>CySA+</td>
<td>CompTIA Cyber Security Analyst</td>
<td></td>
</tr>
<tr>
<td>PenTest+</td>
<td>CompTIA PenTest+</td>
<td></td>
</tr>
<tr>
<td>CASP</td>
<td>CompTIA Advanced Security Practitioner</td>
<td></td>
</tr>
</tbody>
</table>
DOD’s CYBERSECURITY SOLUTION
END USER TRAINING

- At least yearly security briefings
- Raytheon’s “Killing with keyboards”
- Mixed success overall
  - Social media – a necessity for many
  - Smartphones – a necessity for many
  - Family & friends compulsively share

On December 17, 2002, the Federal Information Security Management Act (FISMA) became law requiring all federal agencies to become compliant.

The Defense-wide Information Assurance Program (DIAP) was formed to develop a program and document that would be the guideline for the Directive called DoD Directive 8570. The document was released in 2005.

DoD Directive 8140 was released in 2015. It superseded Dir. 8570.
• DoD Directive 8570/8140 provides the basis for an enterprise-wide solution to train, certify, and manage the DoD Information Assurance (IA) workforce.

• The policy requires Information Assurance technicians and managers to be trained and certified to a DoD baseline requirement.

• The Directive’s accompanying manual identifies the specific certifications mandated by the Directive’s enterprise-wide certification program.
## DIRECTIVE 8570/8140 CERTIFICATIONS

<table>
<thead>
<tr>
<th>IAT Level I</th>
<th>IAT Level II</th>
<th>IAT Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+ CE</td>
<td>CCNA Security</td>
<td>CASP+ CE</td>
</tr>
<tr>
<td>CCNA-Security</td>
<td>CySA+ **</td>
<td>CCNP Security</td>
</tr>
<tr>
<td>Network+ CE</td>
<td>GICSP</td>
<td>CISA</td>
</tr>
<tr>
<td>SSCP</td>
<td>GSEC</td>
<td>CISSP (or Associate)</td>
</tr>
<tr>
<td></td>
<td>Security+ CE</td>
<td>GCED</td>
</tr>
<tr>
<td></td>
<td>SSCP</td>
<td>GCIH</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IAM Level I</th>
<th>IAM Level II</th>
<th>IAM Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP</td>
<td>CAP</td>
<td>CISM</td>
</tr>
<tr>
<td>GSCL</td>
<td>CASP+ CE</td>
<td>CISSP (or Associate)</td>
</tr>
<tr>
<td>Security+ CE</td>
<td>CISM</td>
<td>GSCL</td>
</tr>
<tr>
<td></td>
<td>CISSP (or Associate)</td>
<td>CCISO</td>
</tr>
<tr>
<td></td>
<td>GSCL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CISM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CISSP (or Associate)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GSCL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CCISO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IASAE I</th>
<th>IASAE II</th>
<th>IASAE III</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASP+ CE</td>
<td>CASP+ CE</td>
<td>CISSP-ISSAP</td>
</tr>
<tr>
<td>CISSP (or Associate)</td>
<td>CISSP (or Associate)</td>
<td>CISSP-ISEEP</td>
</tr>
<tr>
<td>CSSLP</td>
<td>CSSLP</td>
<td></td>
</tr>
</tbody>
</table>

39
## DIRECTIVE 8570/8140 CERTIFICATIONS

<table>
<thead>
<tr>
<th>CSSP Analyst</th>
<th>CSSP Infrastructure Support</th>
<th>CSSP Incident Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEH</td>
<td>CEH</td>
<td>CEH</td>
</tr>
<tr>
<td>CFR</td>
<td>CySA+ **</td>
<td>CFR</td>
</tr>
<tr>
<td>CCNA Cyber Ops</td>
<td>GCISP</td>
<td>CCNA Cyber Ops</td>
</tr>
<tr>
<td>CySA+ **</td>
<td>SSCP</td>
<td>CySA+ **</td>
</tr>
<tr>
<td>GCIA</td>
<td>CFR</td>
<td>GCFA</td>
</tr>
<tr>
<td>GCIH</td>
<td>GCIH</td>
<td>GCIH</td>
</tr>
<tr>
<td>GICSP</td>
<td>SCYBER</td>
<td>SCYBER</td>
</tr>
<tr>
<td>SCYBER</td>
<td></td>
<td>CHFI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CSSP Auditor</th>
<th>CSSP Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEH</td>
<td>CISM</td>
</tr>
<tr>
<td>CySA+ **</td>
<td>CISSP-ISSMP</td>
</tr>
<tr>
<td>CISA</td>
<td>CCISO</td>
</tr>
<tr>
<td>GSNA</td>
<td></td>
</tr>
<tr>
<td>CFR</td>
<td></td>
</tr>
</tbody>
</table>
Four categories:

- Technical (IAT)
- Management (IAM)
- System architecture and engineering (IASAE)
- Computer network defender (CND).

Each category has levels based on where the position is located within the overall Information System architecture.
DIRECTIVE 8570.1M: WHO NEEDS THE CERTIFICATIONS?

- **IA Technical:** Anyone with privileged system access performing IA functions at computing, networking or enclave positions.
- **U.S.A. IA Management:** Personnel performing management functions for Govt. systems (e.g. IA Officers)
- **Personnel performing DAA functions** MUST meet baseline training and certification requirements
- **This directive applies to** ALL U.S.A. Govt. departments as well as, contracts for personnel providing IA functional services for U.S.A. DoD information systems (IS)
RIPPLES IN THE POND

- Other Federal Govt. Agencies
- Govt. Programs with Federal Funding
- State Programs
- Local Govt. Programs
- Any organization with Govt funding or THINKS it might have in the future
- State, local organizations are affected too. Think 1981 - the effect of the release of the IBM PC
- CYA effect
SUMMARY

• Cybersecurity skills are in demand (av. $84,000/$96,000)
• Cybersecurity skills are especially in demand in Government organizations
• Salaries are slightly lower, working conditions, benefits, employment stability higher
• In order to get a desired Information Assurance/Cybersecurity position with the U.S. Government or any organization that might work with the U.S. Government, you need to know about and comply with Directives 8570/8140
• www.opm.gov – worth looking at
QUESTIONS?

Questions?
Dr. David Anderson
• Dept. of Computer Information Systems, Triton College, River Grove, IL 60171
• davidanderson@triton.edu

Dr. Karl Reimers
• Tillman School of Business, University of Mount Olive, Mount Olive, NC 28365
• kreimers@umo.edu
REFERENCES

References


MOC Focus Groups, 2010. Mount Olive College, Mount Olive, NC.


REFERENCES

References


https://www.youtube.com/watch?v=RcyZyw9uYf8
https://www.youtube.com/watch?v=8yedqItGXLs