



GENEDGE

innovate. compete. grow.

Making Virginia the World Leader in Cyber Security

New College Institute - Martinsville VA

March 23, 2015

Bill Donohue

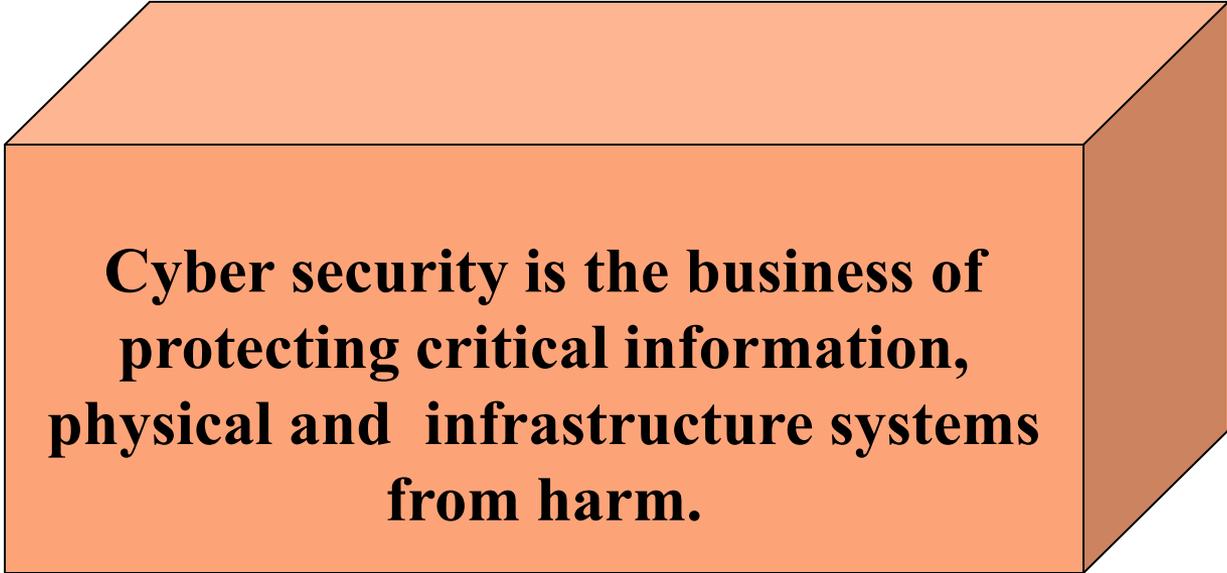
The Cyber Security Failure that Changed History



The Enigma Machine code breaking capabilities advanced by the British at Bletchley Park were Instrumental in saving Western Civilization.....



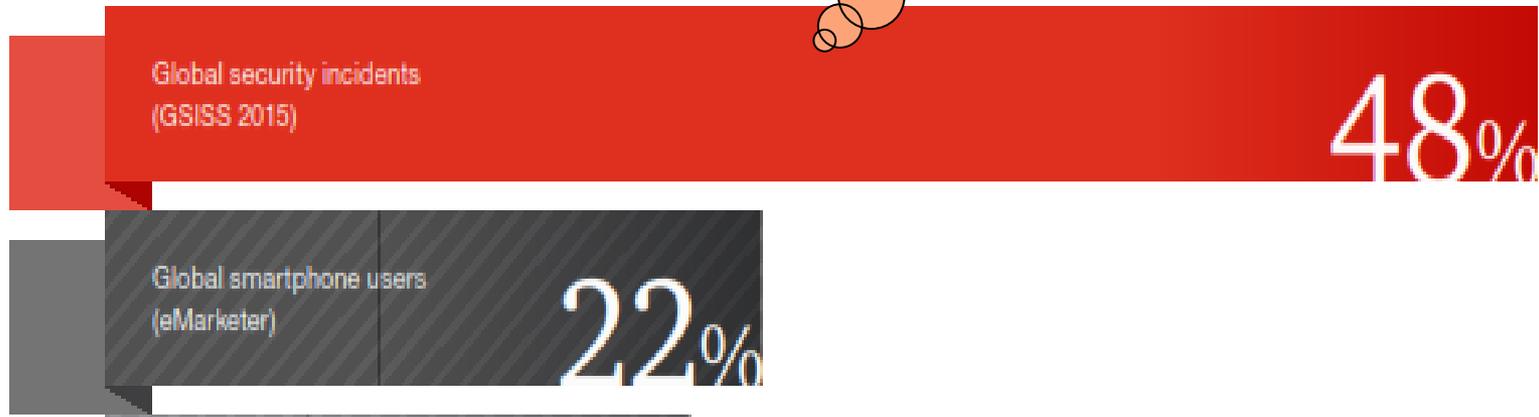
What is Cyber Security?



Cyber security is the business of protecting critical information, physical and infrastructure systems from harm.

How Fast is the Problem Growing?

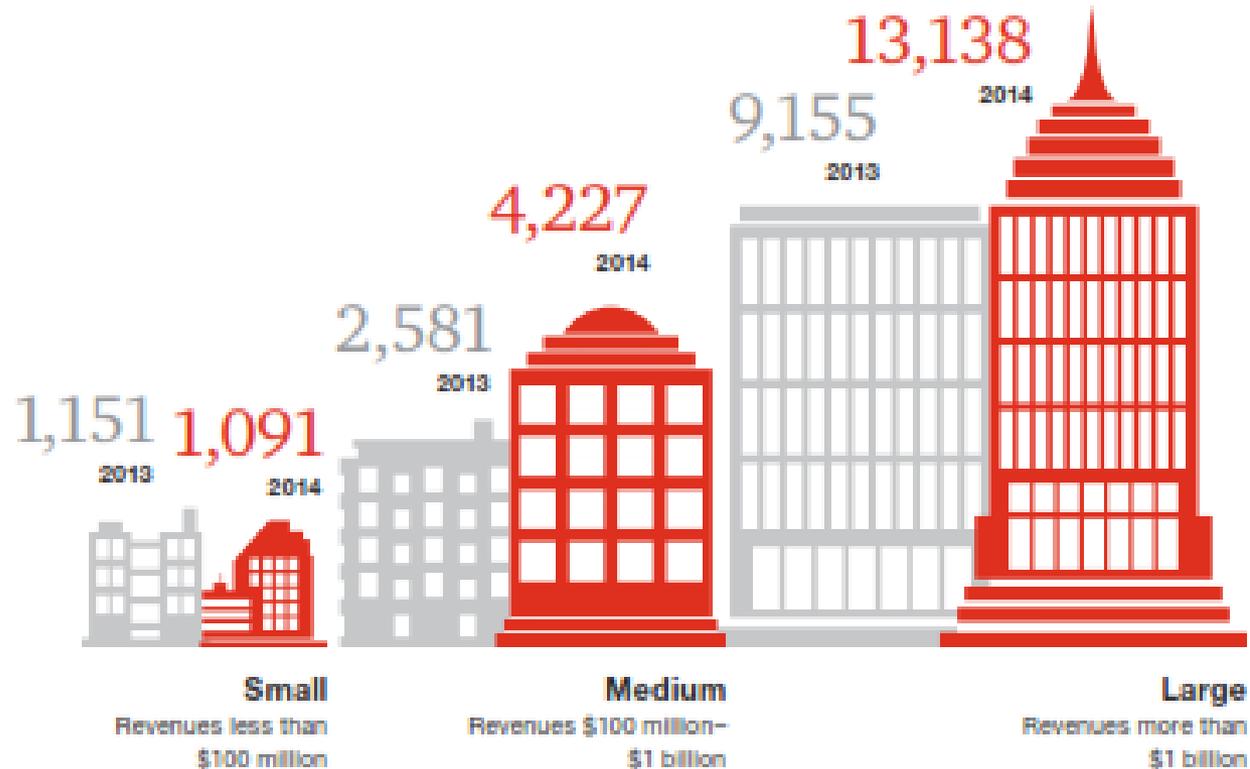
U.S. companies and public sector units raised computer security spend to an estimated \$89.1 billion in the fiscal year ending October 2013, more than double the 2006 level.



While it is a Problem, it is also a High Growth Market

Sources: Price Waterhouse Coopers Global Information Security Survey 2015, Ponemon Institute, analyzed by Bloomberg.

Company Size affects Rates of Attack



Source: Price Waterhouse Coopers Global Information Security Survey 2015

US Critical Infrastructure – 2014 Reported Attacks

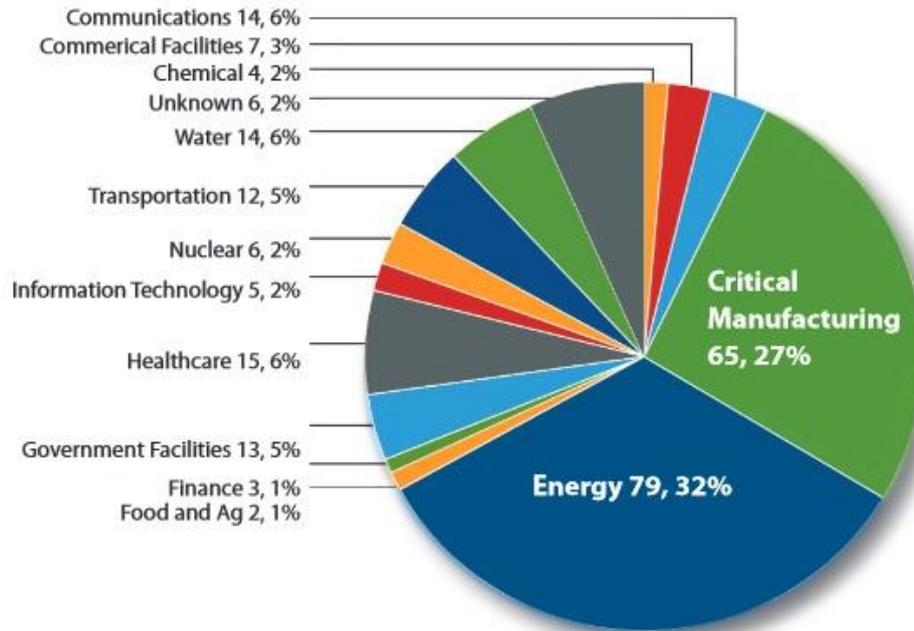


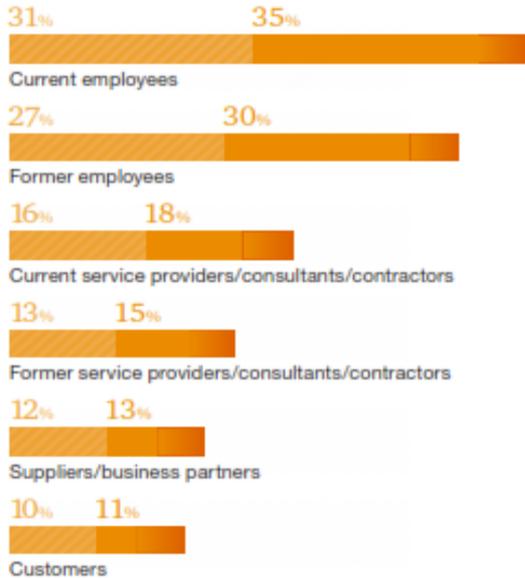
Figure 1. FY 2014 incidents reported by sector (245 total).

40% of these Attacks had No Known Access Vector

- **Unauthorized access and exploitation of Internet facing ICS/Supervisory Control and Data Acquisition (SCADA) devices**
- **Exploitation of zero-day vulnerabilities in control system devices and software**
- **Malware infections within air-gapped control system networks**
- **SQL injection via exploitation of web application vulnerabilities**
- **Network scanning and probing**
- **Lateral movement between network zones**
- **Targeted spear-phishing campaigns**
- **Strategic web site compromises (a.k.a., watering hole attacks.)**

Sources of Threats – 2013 vs 2014

Insiders



Outsiders



Source: Price Waterhouse Coopers Global Information Security Survey 2015

Where do Attacks Surface?



Government



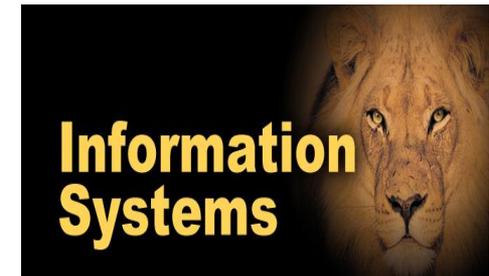
Infrastructure



Physical Devices



Retail Credit



Where do Attacks Surface?



Industrial Control Systems



The NIST Cybersecurity Framework

President issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013

NIST created a voluntary, collaborative Framework for use by the Nation on February 12, 2014



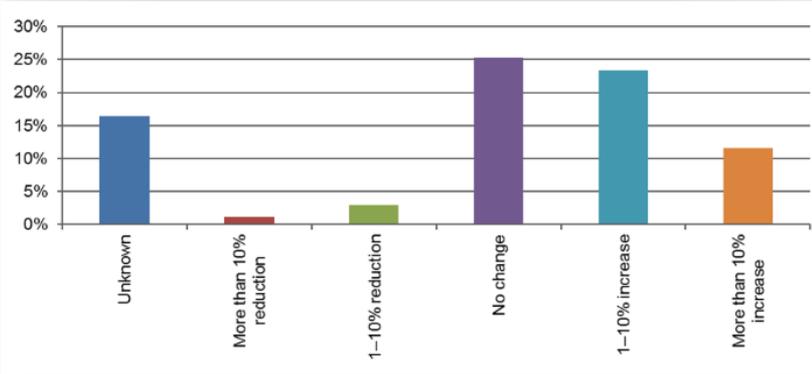
Framework Details – think ISO 9000

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: NIST Cyber Security Framework version 1.0

Job Growth in Cyber Security

What is the projection for security staffing over the next 12 months?



With 35% of companies reporting > 10% annual staff additions, and 60% of professionals with less than 10 years experience, growth will be rapid in the future

How many years of experience do you have in IT security?

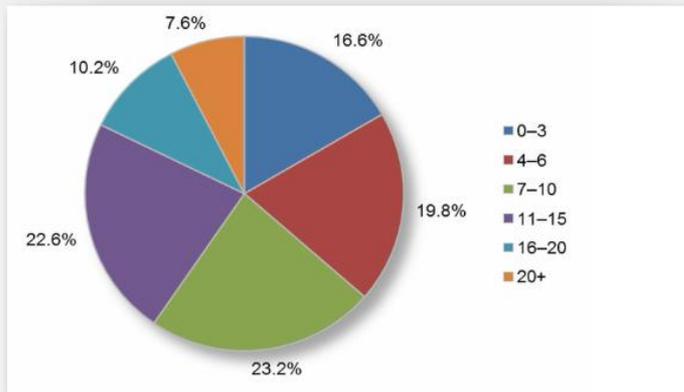
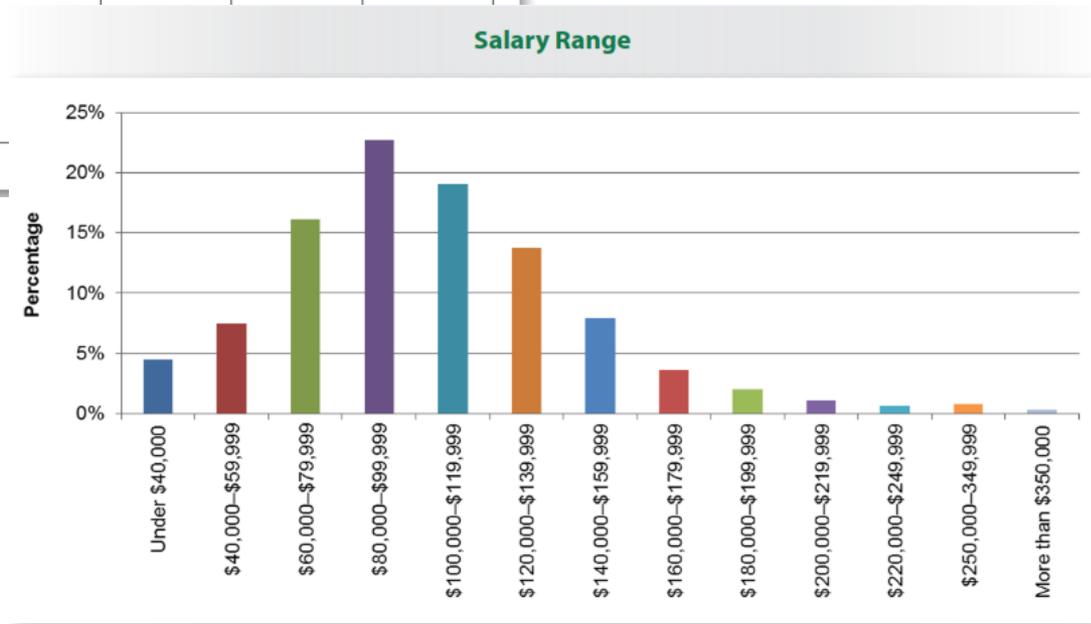


Figure 6. Respondents' Years of Experience

Source: SANS survey, May 2014

Job Titles and Salaries

Avg. Annual Income exceeds \$102,000



Source: SANS survey, May 2014

What Drives Success?

What are the biggest contributing factors to your career success so far?

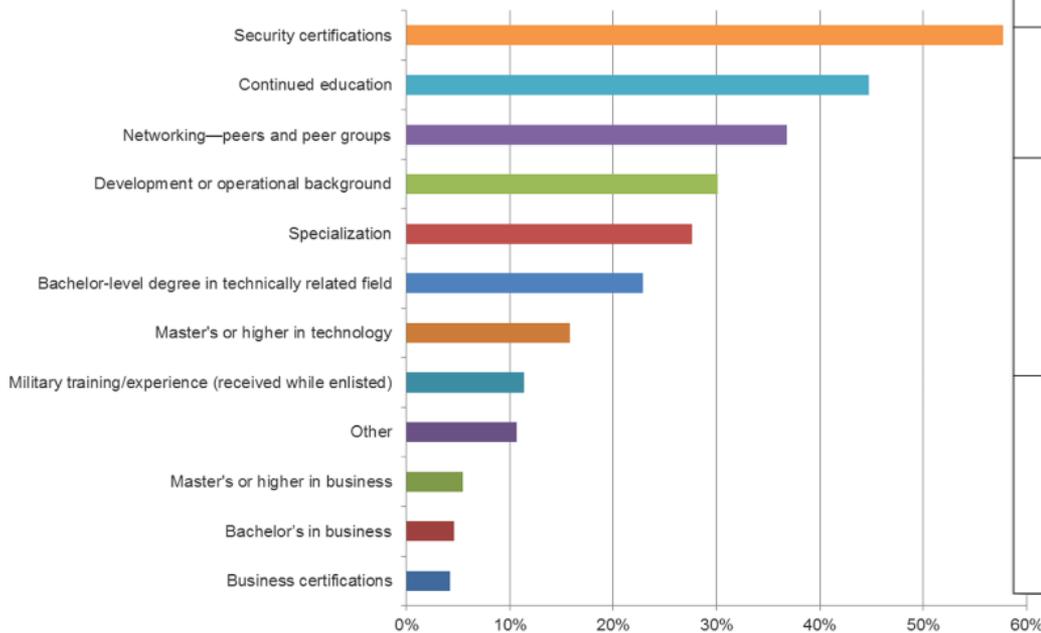
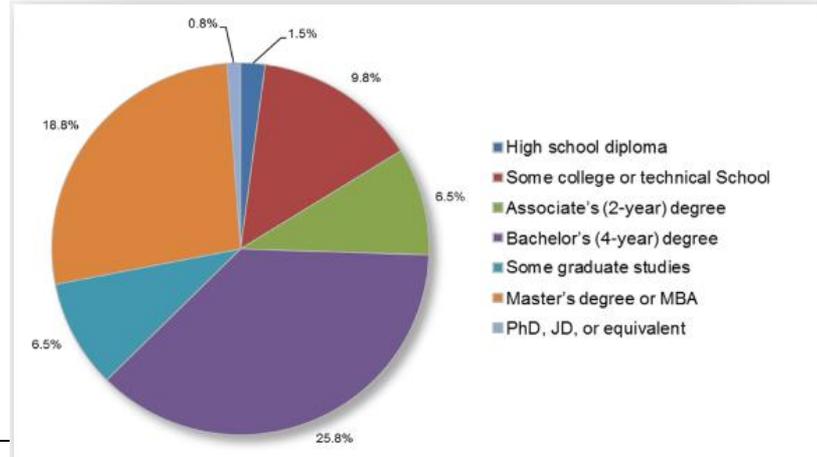


Table 6. Value Proposition of Certification

Value Tier	Certification
First	GIAC Security Expert (GSE)
	ISC(2) Certified Information Systems Security Professional (CISSP)
Second	GIAC Certified Forensics Analyst (GCFA)
	GIAC Penetration Tester (GPEN)
	GIAC Industrial Cyber Security Professional (GICSP)
Third	GIAC Certified Incident Handler (GCIH)
	ISACA Certified Information Systems Auditor (CISA)
	GIAC Security Essentials Certification (GSEC)
	GIAC Certified Intrusion Analyst (GCIA)
	GIAC Security Leadership Certification (GSLC)
Fourth	CompTIA Security+
	ISC(2) Certified Cyber Forensics Professional (CCFP)
	EC-Council Certified Ethical Hacker (CEH)
	Cisco Certified Network Professional (CCNP)
	Cisco Certified Security Professional (CCSP)

Highest Level of Education



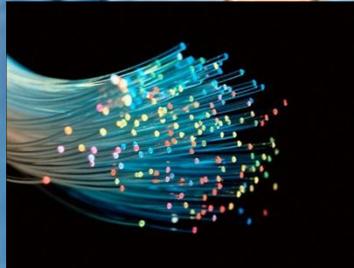
Source: SANS survey, May 2014

Why Virginia?



Domestic Markets Expansion Program
DMEP VIRGINIA

57 Higher Ed
Institutions
offer Quality
IT degrees



Source: FORBES Magazine



Thank You.

www.genedge.org