Cybersecurity Strategy for Business

Jack Britton

$~: whoami

- Husband, Dad, and Marine Veteran
- Undergraduate and Masters of Science in Cybersecurity
- Fortune 500
  - Consulting
  - Risk Assessments
  - Programs Development
  - Ethical Hacking, “Penetration Testing”

Why invest in Cyber Security Strategy?

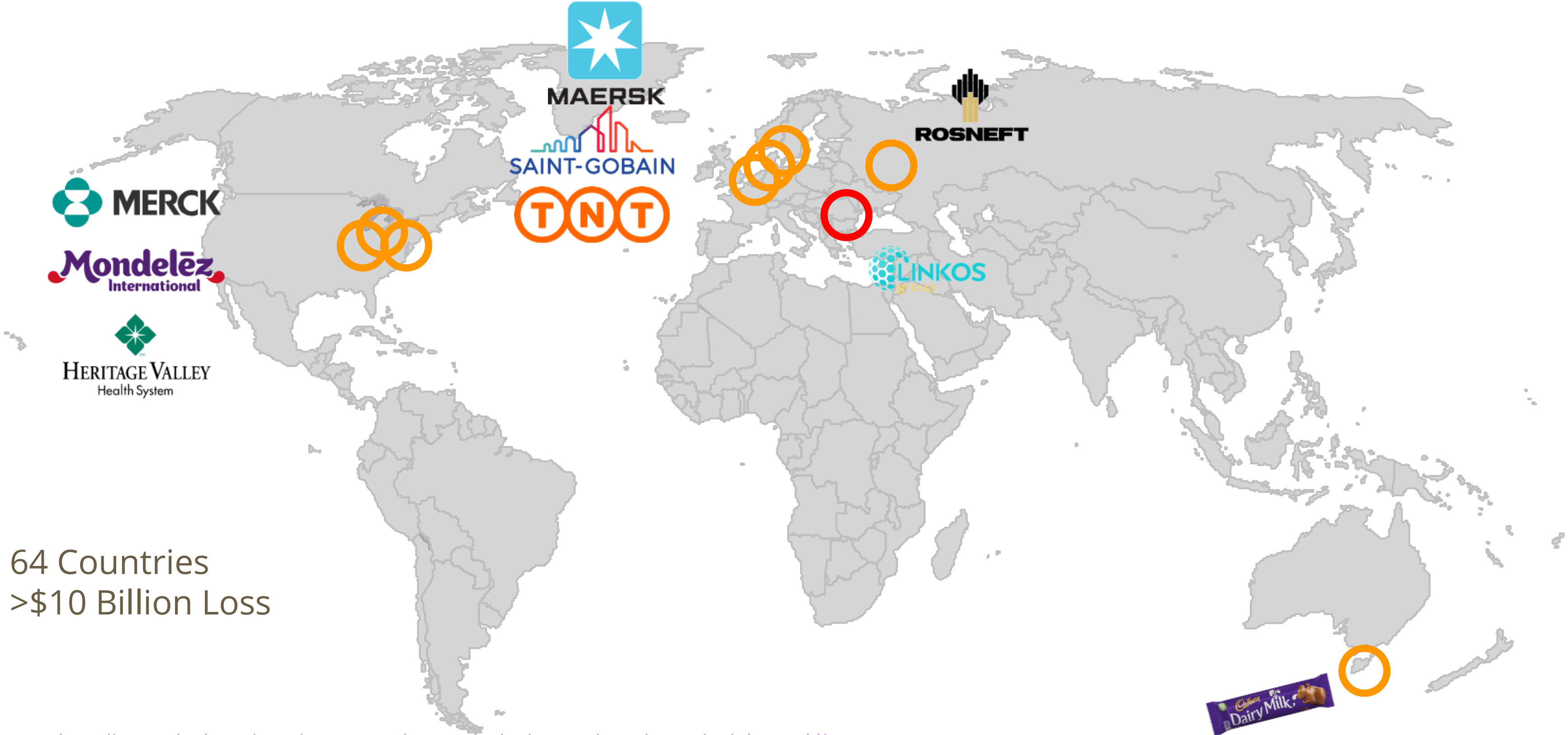
- Protect **People**
- Improve Business Operations
- Protect Business “Assets”
- Hedge the Breach “Expense”
- Protect Business Reputation
- Gain a Competitive edge

I don’t care if this security software was a bargain; it shouldn’t reply with “close enough” when I enter the wrong password.

CartoonStock.com

Business and Consumers inextricably share technology risks.

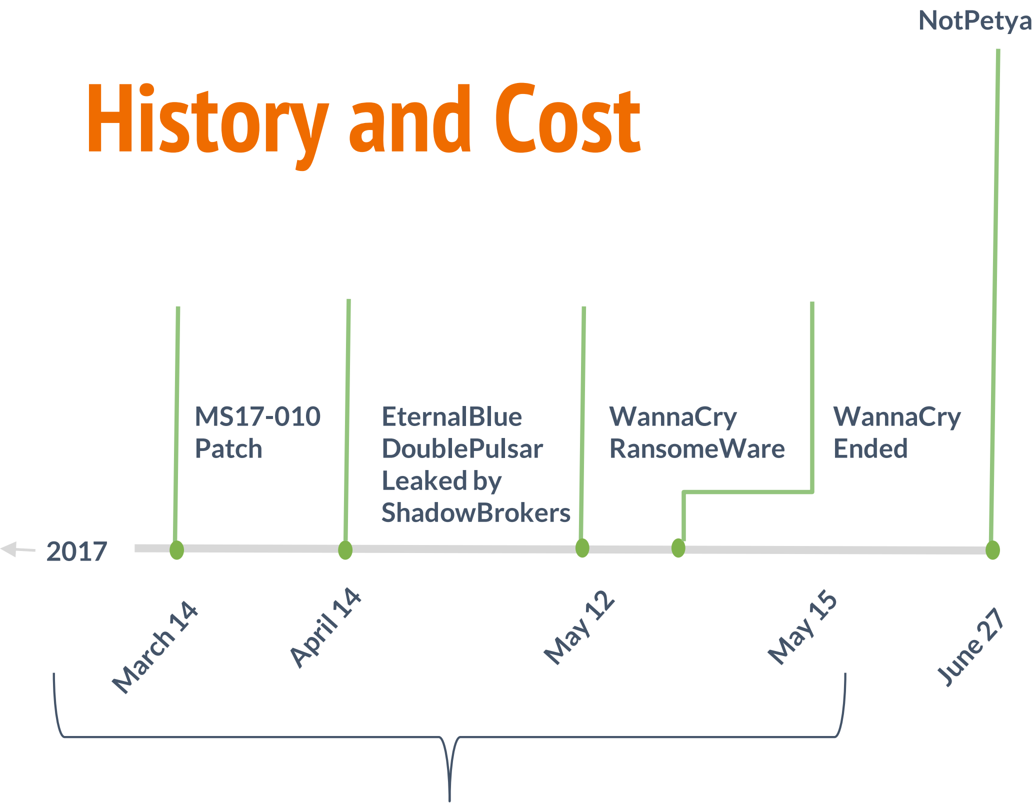
Not Convinced, Remember NotPetya?



64 Countries
>$10 Billion Loss

Reference: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

History and Cost



NotPetya

MS17-010 Patch

EternalBlue DoublePulsar Leaked by ShadowBrokers

WannaCry RansomeWare

WannaCry Ended

2017

March 14

April 14

May 12

May 15

June 27

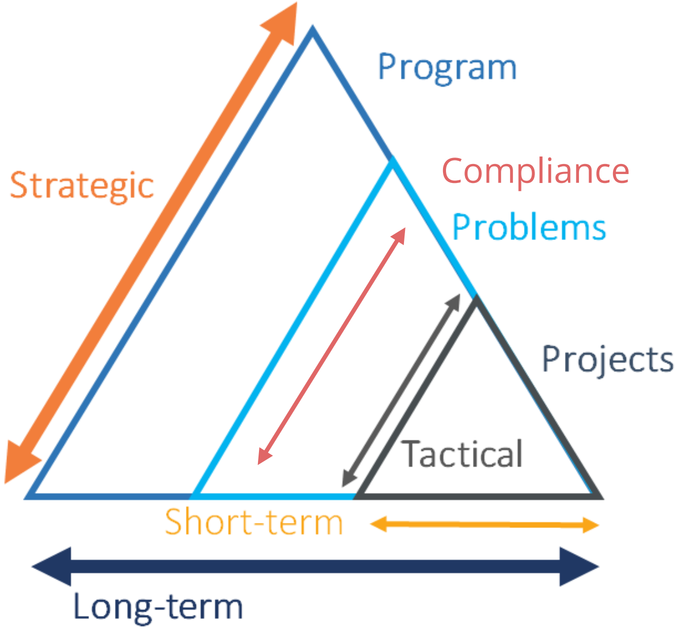
Russian state sponsored hacking teams Fancy Bear and Sandworm attack Ukraine

Vulnerability and Patch Management?

LINKOS group	Family Software Company Ground Zero
MAERSK	Export Logistics Company $300,000,000
MERCK	Pharmaceutical company $870,000,000
Mondelēz International	Export Logistics Company $188,000,000
Heritage Valley Health System	Medical Industry $...
SAINT-GOBAIN	Manufacturing $230,000,000
TNT	Courier Delivery Service $400,000,000
ROSNEFT	Oil Company $200,000,000

What is a Cyber Security Strategy?

Tactical Projects	Strategic Program
Reactive	Proactive
Smaller Scope	Larger Scope
Short-Term	Long-Term
Executing	Planning & Executive
Checking the Box	Effective solution
Expensive	Cost saving



Cyber Security VS Compliance

Business function(s)

intended to prevent unauthorized access or misuse of electronic systems and data

Cyber Security

- Decisions driven by “Risks”
- Opportunity to measure **Risk vs Reward**

Compliance

- Decisions driven by **Regulations** or **Contract**
- Business **Risk** when in-scope

“**Risk**” is the **possibility** of **losing** something of **value**

General Data Protection Regulation (GDPR)

New Regulation

Designed to give EU Citizens more control of their data

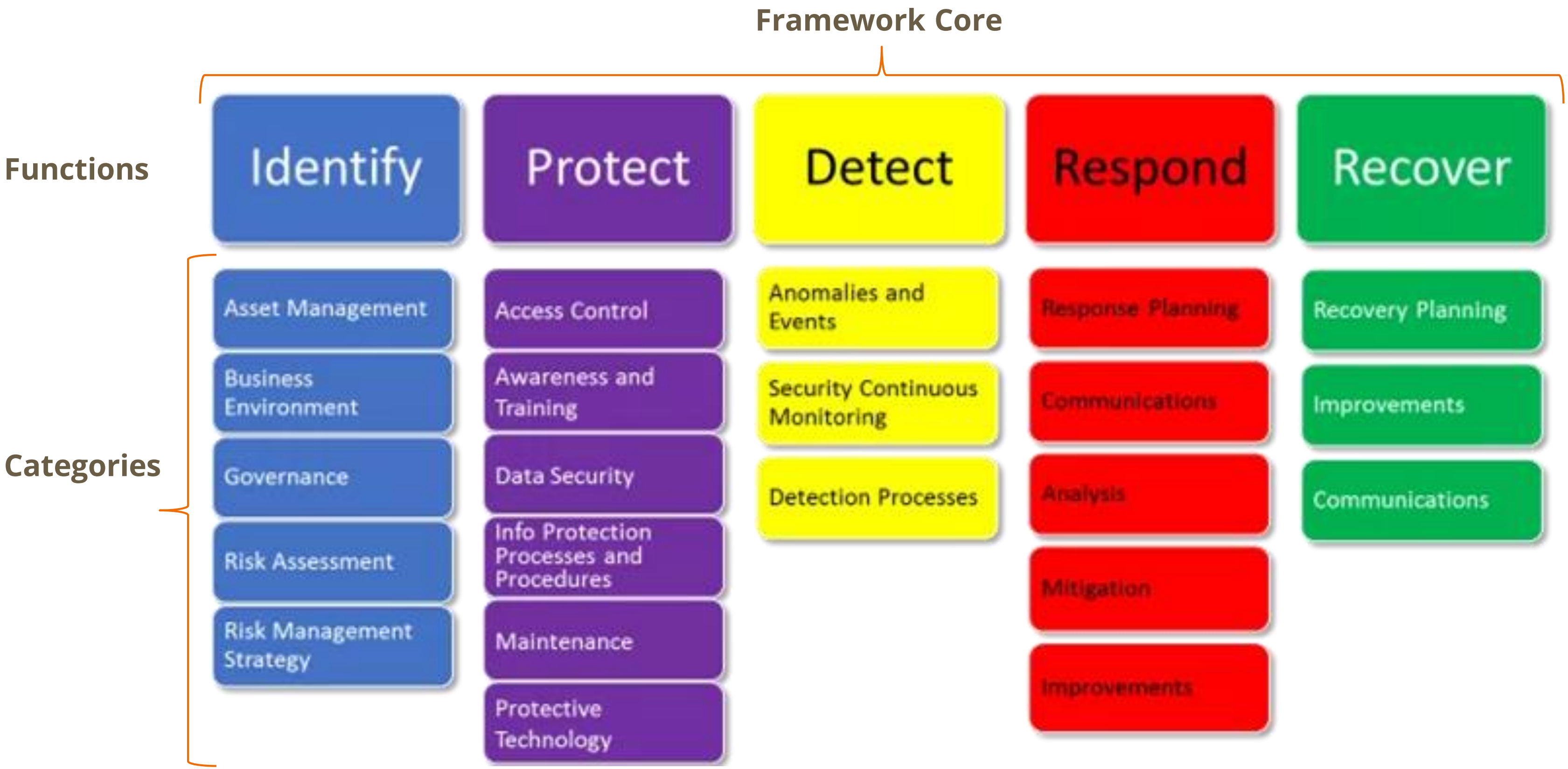
- **Controllers** and **Processors** of EU Citizens Personal Data
    - Regardless of location
    - Target EU citizens for goods or services
    - Behavior monitoring

- **Fines**
    - **€10 million** or **2% worldwide annual revenue** of the prior financial year
    - **€20 million**, or **4% worldwide annual revenue** of the prior financial year

Do Remember

1. Privacy by Design - controls
2. Pseudonymization and Encryption Data
3. Customer - “data subject” - rights
4. Prepare for a breach

NIST Cyber Security Framework



Framework Core

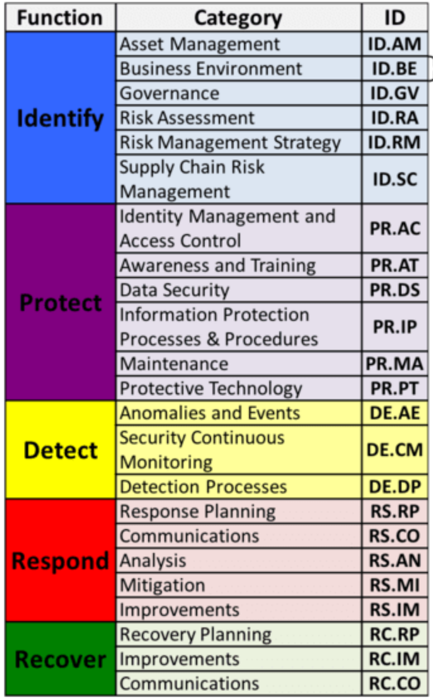
Functions

Categories

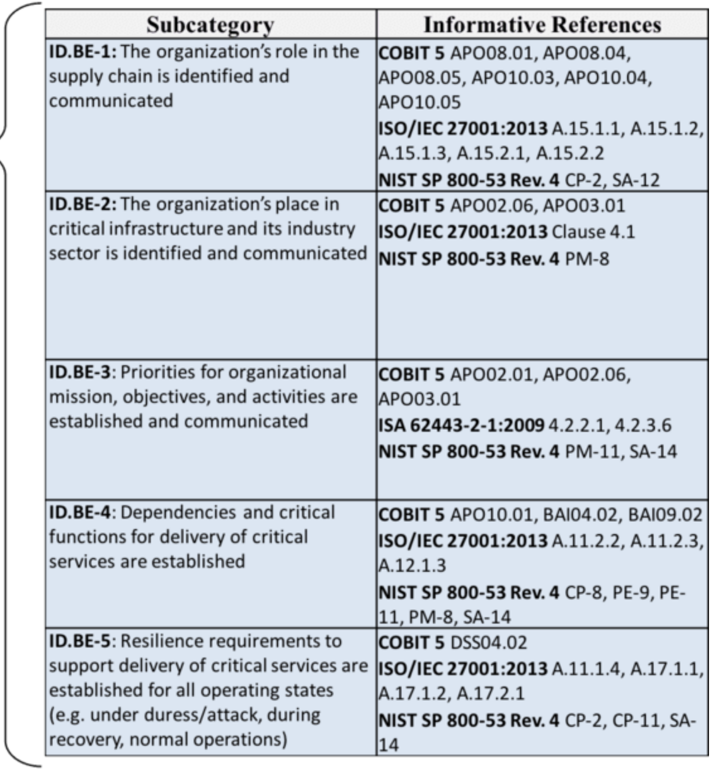
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Reference: https://www.nist.gov/cyberframework

Assess Cyber Security Activities



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



Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Activities measured against Guidelines

Not Aware	Partial	Risk Informed	Repeatable	Adaptive
0	**1**	**2**	**3**	**4**
No awareness , No knowledge	Informal Practices; limited awareness; no cybersecurity coordination	Management approved processes and prioritization, but not deployed organization-wide; high-level awareness exists, adequate resources provided; informal sharing and coordination	Formal policy defines risk management practices processes, with regular reviews and updates; organization-wide approach to manage cybersecurity risk, with implemented processes; regular formalized coordination	Practices actively adapt based on lessons learned and predictive indicators; cybersecurity implemented and part of culture organization-wide; active risk management and information sharing.

	Category	ID	Subcategory		BU1	BU2	BU3
Identity	Business Environment	ID.BE	ID.BE-1	The organizations role in the supply chain is identified and communicated.	1.31	3.05	2.00
			ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated.	2.03	1.40	0.05
			ID.BE-3	Priorities for organizational mission, objectives, and objectives, activities are established and communicated.	2.06	0.33	4.00
			ID.BE-4	Dependencies and critical functions for delivery of critical services are established	2.07	3.50	3.85
			ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	2.08	1.35	1.05

Filling Cyber Security Gaps = Service Offerings

Security Strategy and Program

Offensive Security

Security Ops & Incident Response

Identity and Access Management

Data Security

Endpoint Security

Application and Web Security

Infrastructure/Network Security

Cloud, Mobile, and IoT Security

Managed Security Services

Questions and Answers

Invest in a Cybersecurity Strategy

Jack Britton - jack@brittonjr.com
LinkedIn - https://www.linkedin.com/in/jackrbritton/