Agenda

- Introductions
- Healthcare Cybersecurity - Let’s Make it Contagious!
- Cybersecurity saves money – and lives
- The “battle” between operations and security
- The weakest link is the one that will break first
- Detecting compromised (including shared) credentials
- 3rd party access compromise
- Theft and loss prevention (hardware, data, identity)
- Cybersecurity training at all levels
- Cybersecurity considerations in purchasing
- The more you design in, the less you have to glue on
- Doctors and Nurses aren’t the only experts in the Medical Treatment Facility
- The shift from fortification mentality to resiliency and restoration
- Conclusion
Introduction to General Dynamics

Formed in 1952 with a lineage back to 1899:
- Aerospace – Jet Aviation & Gulfstream
- Combat Systems - Land Combat Vehicles & Munitions
- Marine Systems – Surface Ships & Submarines
- Information Systems and Technology (IS&T)

AEROSPACE

$8.8 billion
16,500 Employees

COMBAT SYSTEMS

$5.6 billion
14,500 Employees

MARINE SYSTEMS

$8.0 billion
21,500 Employees

INFORMATION SYSTEMS AND TECHNOLOGY

$9.0 billion
43,500 Employees
General Dynamics Information Technology (GDIT)

One of two operating Companies that comprise GD’s Information Systems and Technology (IS&T) Family.

- Enterprise IT system development and integration
- Enterprise Cyber operations & management, security, and engineering
- Mission support services
- Simulation and training
Healthcare Cybersecurity - Let's Make it Contagious!

• Explosive growth in networked medical devices (mobile, fixed, specialized) and long term data storage requirements
• Use of data mining to provide value-based care
• Finding efficiencies in the metrics
• Maximizing patient care
• Minimizing IT security risks
Cybersecurity Saves Money – and Lives

- Electronic Health Records (EHRs) are “gold” – they are of monetary and life value
- How much does it cost? – A LOT
  - Average Cost = $3,149,000
  - Detection Cost = $610,000
  - Notification Cost = $560,000
  - Regulatory Cost = $1,979,000
  - Hidden Cost = ?? (Lost reputation, future revenue, employees, etc.)
- Death by hack? Yes, it can happen!
  - E.g., Infusion pumps, automated medication, pacemakers…
  - Multiple devices feeding/accessing EHRs increases risk
- Protecting EHR data can lower / avoid costs
The “Battle” Between Operations and Security

- How to get to “Yes”; Cybersecurity supporting Operations
- The common goal: Usable and Secure
- The fight over resources: people, budget, space, time, etc.
- Architecture growing to incorporate more end points; attack surface is increasing
- Long-term data silos at risk – not just today’s data
- Security and Operations working together to ensure proper business processes are in place for facilities, infrastructure, and personnel
  - For example, risk of inadequate new-employee security training when in a rush to fill vacancies
The Weakest Link is the One That Will Break First

• The *Human Factor* (i.e. the 8th layer of the OSI model)
• Proliferation of wireless devices are subject to jamming and sniffing
• Mix of legacy and special requirements drive up support costs
  • Example: FDA Systems
• Inaccurate, incomplete, out-of-date inventory asset data
• Poor or nonexistent configuration and change management
• Gaps in the end-to-end situational awareness – what you don’t know **WILL** bite you!
• Stove-piped systems that are not interoperable
• Single points of failure
• And…
Detecting Compromised (Including Shared) Credentials

- The #1 leading cause of security breaches…
- Mitigation = strong automated password management
  - Change defaults on everything
  - Password expiration policy
  - Detect multiple log-ons
  - Password clipping (lock-out after x wrong tries)
  - Something you have, are, know – and “be”
- Authentication - Authorization – Accountability
- Jackpots - passwords stored in (or written on) medical supply cabinets; default hard-coded passwords
- Post-it notes are not a secure password cache
- Single Sign On is GREAT – but also dangerous
3rd Party Access Compromise

- Due to increased concentration on the “Core” business -
  - Food service, logistics, janitorial, physical security are often outsourced
  - Emergency rooms are even outsourced
  - So - consider Security-based SLAs with 3rd party vendors

- Who do you trust? Look what happened at:
  - Target (BMS)
  - Lowes (PoS)
  - Google (BMS)

- Watch for the TOR
  (encrypted traffic that doesn’t belong)
Theft and Loss Prevention (Hardware, Data, Identity)

- Data leak / loss prevention
- WIFI vulnerabilities
- Snapchatting surgeries
- Increasing inappropriate Facebook and social media use
- HIPAA considerations for data loss / leakage
  - NIST/SP 800-66 HIPAA Security Rules
- Hardware Protection Considerations
  - Encryption
  - RFID, GEO tracking, fencing
  - Remote wipe
  - Improper disposal/data sanitation
Cybersecurity Training at all Levels

- Teaching the users to be observant
  - Test on what you teach! (e.g., internal phishing program)
- Teaching the administration how to respond
- Teaching auditors how to inspect
- Teaching *everyone* to put cybersecurity in the forefront
Cybersecurity Considerations in Purchasing

• Before purchasing:
  • Have the requirements been identified?

• During purchasing:
  • Does the vendor meet requirements, including security?
  • Will you lease, purchase, or borrow?
  • What is the Total Cost of Ownership?
  • Was a cost benefit analysis performed?

• After purchase:
  • Have you developed a lifecycle replacement plan?
The More You Design in, the Less You Have to Glue on

• Include security in the planning phase
  • Properly identify requirements

• Incorporate proven and tailorable frameworks, e.g.:
  • ITIL® (formerly IT Infrastructure Library)
  • Information Technology Systems Management
  • Information Technical Architecture Framework
  • Sherwood Applied Business Security Architecture

• Implement a formal configuration control board (CCB)
  • Senior management oversight
  • Department heads formally vote for products / systems
    • IT Security gets a voice
  • All system changes are identified
Doctors and Nurses Aren’t the Only Experts in the Medical Treatment Facility

- Issues moving from pen & paper charts to hyper-converged networked devices and EHRs
- Doctors, Nurses, and IT experts working together to enable and verify knowledge-based decisions
  - “Medical Infomatics”
- Medical IT innovation – a brave new world
  - Microchips modeling clinical trials
  - Wearable technology like Google Glass
  - Star Trek tricorder & biomedical scanners
  - 3D printed biological materials
  - All great stuff – but don’t forget Security!
The Shift From Fortification Mentality to Resiliency and Restoration

- Set it and forget it mindset – a disaster waiting to happen
- Protect, Monitor, Analyze, and Respond
  - Enclave Hardening – put up the best defense you can
  - Continuous Monitoring Strategy – you have to be watching
  - Incident Response – have a proven plan on how to respond
- Defenders have to be right 100% of the time – attackers only have to be lucky once!
- You **will** be breached! Plan for **Resiliency** from the start
- Detect + Isolate + Recover + Restore = Resiliency
- Lessons learned
Closing Questions, Caveats, & POCs

• Opinions and statements herein are those of the author and do not represent official statements, positions, or policies from General Dynamics, General Dynamics Information Technology, or any other institution.

• Information presented herein is all public source.

• The use of trade names does not constitute any endorsement of such product or service.

• Any use of this presentation without written permission from the author is prohibited.

• For further information, please refer to:
  • www.GD.com
  • www.GDIT.com
  • Joseph.Walker@gdit.com