Cybersecurity - Integrating People, Process and Technology
About the Speaker

Anil Chacko, MBA, PMP, CISM, CRISC
Managing Director, SMART DEVINE

Anil has over 25 years of experience in Technology and Information Security. Mr. Chacko was responsible for creating a guiding vision for resuming business activities and sustaining revenue generation through disruptive events. He has led teams to produce disaster recovery action plans and to launch recovery sites with real-time server replication.

Anil has spent the past 15 years working with different aspects of Information Security. His experience includes safeguarding systems and data by conceptualizing strategy and leading IT team and consultants to implement a security framework including processes, procedures, and training for controlling and monitoring security.

Mr. Chacko has a BS in Computer Science and an MBA in Public Accounting from St. John’s University. He is a Lean Six Sigma Green Belt and has a Master Certificate in Business Process Management. Anil is an active volunteer with IASA and has spoken at the conference several times. He can be reached at achacko@smartdevine.com or at 917.348.1011.
Am I Vulnerable to a Cyber Attack?
Cyber Security vs Information Security

- **Cyber Security** is the use of various technologies and processes to protect networks, computers, programs and data from attack, damage or unauthorized access.

- **Information Security** is protecting information from unauthorized access, use, disruption, modification or destruction regardless of how the information is stored – electronic or physical.
How the threat has changed

- IT Assets within the 4 walls
- Single entry point
- Restricted access
- Continuous Monitoring
How the threat has changed

- Equipment within the 4 walls
- A new entry point – Connection to the outside world via internet
- Restricted access?
- Continuous Monitoring?
How the threat has changed

- Equipment within the 4 walls
- Multiple entry points (Internet, VPN, BYOD, 3rd Party Service Providers)
- Restricted access ??
- Continuous Monitoring ??
Taking a holistic approach

- People
- Process
- Technology

Get the right balance of People, Process and Technology and the stool will be solid and well balanced, concentrate only on technology and the stool will be wobbly.
PEOPLE

- Ensure Senior Management buy-in and commitment. *Without this you will fail.*

- Employ the right people with the right attitude, experience and qualifications.

- Train your people and test them periodically

- Rewards and recognition to reinforce behavior

  **Make security a cultural focus of the organization**
PROCESS

- Build these first and then select the Technology
- Clearly communicate the established processes within the organization
- Train the People on the Processes and get their buy-in to see 'what's in it for them'
- The processes should be aligned to the organizations risk tolerance and business objectives
TECHNOLOGY

- Understand how the technology works and the exposure it creates
- Monitor changes in technology and deploy effective tools
- Ensure software patches and updates are done on a timely fashion
- Continuously monitor the log files against an established baseline
Standards and Frameworks

- **ISO** – International Organization for Standardization
  - 27000 Series – ISO27K

- **NIST** – National Institute for Standards and Technology
  - Special Publication 800 Series
  - Cybersecurity framework

- **CoBIT** – Control Objectives for Information and Related Technology

- **ITIL** – Information Technology Infrastructure Library
Government and Industry Regulations

- Government Regulations
  - HIPAA (Health Insurance Portability & Accountability Act)
  - GLBA (Graham Leech Bliley Act)
  - SOX (Sarbanes Oxley Act)
  - FISMA (Federal Information Security Management Act)
  - Red Flags Rule

- Industry Regulation
  - PCI-DSS
Information Security Triad

- Confidentiality
- Integrity
- Availability
NIST Cybersecurity Framework

5 Concurrent and Continuous Functions

- Identify
- Protect
- Detect
- Respond
- Recover
Identify the assets or resources that support critical functions and risk related to these assets.

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

- Data Security
- Access Control
- Information Protection
- Awareness and Training
- Processes and Procedures
- Protective Technology
- Maintenance
Develop and implement the appropriate activities to identify the occurrence of cybersecurity event.

- Security Continuous Monitoring
- Anomalies and events
- Detection Processes
Develop and implement the appropriate activities to take action regarding detected cybersecurity event.

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements
Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

- Recovery Planning
- Improvements
- Communications
Thank you!
Shawn Nelson
Director, Information Security, Glatfelter Insurance Group

- Shawn Nelson has been the Director of Information Security for Glatfelter Insurance Group since 2012. In this position, Shawn is responsible for maintaining an enterprise wide information security program and oversees all information security projects. Prior to this position, Mr. Nelson served as Director of Network Operations and was responsible for core infrastructure and network security. He started at Glatfelter Insurance Group in 1993 as a Network Technician, and has gained experience from both a technical and business perspective in these roles.

- He can be reached at snelson@glatfelters.com or at 717.741.7847
Who We Are

Glatfelter Insurance Group (GIG)

- Established 1951
- One of the largest privately owned insurance brokers in the United States
- 500+ associates serving 40,000 clients
- Retail and wholesale operations
- Insurance products in all 50 states and Canada
- Niche markets, such as Firefighters, Hospice and Senior Living organizations, Municipalities, Churches, and Schools.
Vision – Threat Landscape

- Strategic change was needed
  - Data Breaches were on the rise
  - Malware infections were increasing
  - Cloud services were becoming mainstream
  - Mobile devices (personal and corporate)
  - Remote workers
What’s Needed

- Establish - Information Security Program
Plan The Structure

- CEO
  - CIO
    - Application Architecture
    - Infrastructure
    - Information Security
    - Application Development
    - Data Warehousing
Establish Your Base Camp

- Perform a “Gap Analysis”
  - Where are you today
  - Where do you want to be

- Determine regulations/compliance

- Identify strategic objectives/goals
  - Policies
  - Technologies
  - People
Base Camp GIG

- Performed an internal assessment – ISO & NIST
- Performed a 3rd party assessment
- Ran vulnerability scans
- Perform a 3rd party penetration test
- Identified “Blind Spots”
Select Your Equipment (Technology)

- Easily managed with a small group
- Can you identify abnormal behavior
- Do you have visibility in to your network/systems
- Can you perform historical analysis
- Can you recover/restore
Equipment Selection GIG (Technology)

- Tiered or layered vendors at the perimeter
- Focused on logging, auditing, alerting
- Implement DLP and IPS
- Implemented Vaulting Technology
  - (Privileged Accounts)
- Implemented encryption
What’s The Plan (Processes)

- Incident Response Plan
- Policies (security, mobile devices, social media)
- Procedures (malware, separations)
- Standards (Encryption)
The Plan GIG (Processes)

- Created an Incident Response Plan
  - Data breach, malware/virus infections/lost/stolen equipment
  - Executive communication plan & tactical plan

- Revised standards (contracts, encryption)
  - Cloud services, consultants, auditors
  - Data breach clauses, US hosting, off loading data

- Revamped policies & procedures
  - Mobile devices, security, separations, data governance
Train The Team (People)

- People – Awareness (Most Important)
  - Build a relationship “trust”
    - (not trying to make their job difficult)
  - Educate on the “why”
  - Don‘t be seen as a business road block!
    - ShadowIT - IT systems and solutions built and used inside organizations without explicit organizational approval
Team GIG (People)

- People – Awareness
  - Phase 1 – IT
    - Threat landscape presentation
    - Technologies presentation
    - Phishing test – gave out fighting fish
  - Phase 2 – Executive Management
    - Customer impact (ability to process claims)
    - Brand impact / reputation
    - Legal / financial impacts
    - Roadmaps
    - Maturity model
Team GIG – (People)

• Phase 3 – Associates
  • Infosec alerts
  • Awareness sessions
  • Explain the “why”
  • Awareness intranet site
  • Infosec hotline
  • Be a partner/advisor not a cop!

MAKE IT PERSONAL.
Are We There Yet?

- Measure your success
  - Metrics
  - Strategic goals
  - Multi-year roadmap
  - Vulnerability scans
  - Annual penetration testing
  - Patch management
What Did We Learn?

- Do the basics well
  - Passwords, permissions, patches, awareness

- Be a strategic partner / advisor
  - Balance usability & security
  - Understand the business needs

- Organization culture changes slowly

- Protect the data
Please Complete the Session Evaluation Form on the Conference App