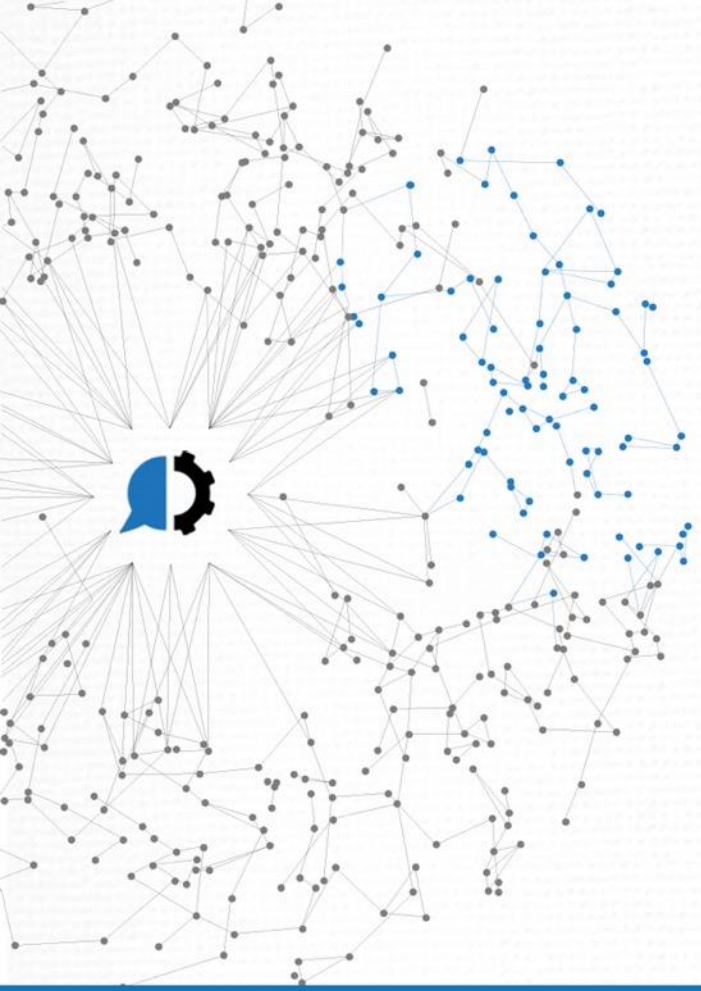


Meeting Compliance Requirements

GoAnywhere

Introductions

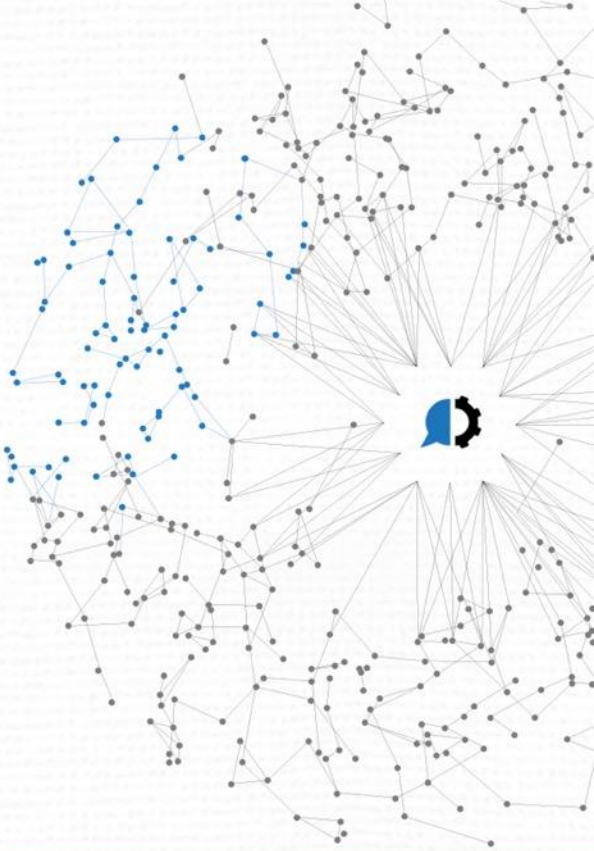
Dan Freeman

Senior Solutions Consultant

CISSP

Agenda

1. What is Compliance
2. Costs of non-compliance
3. Regulations/Laws/Standards/Frameworks
4. What can you do?
5. GoAnywhere secure solutions - Demo
6. Q&A



UP NEXT

Compliance

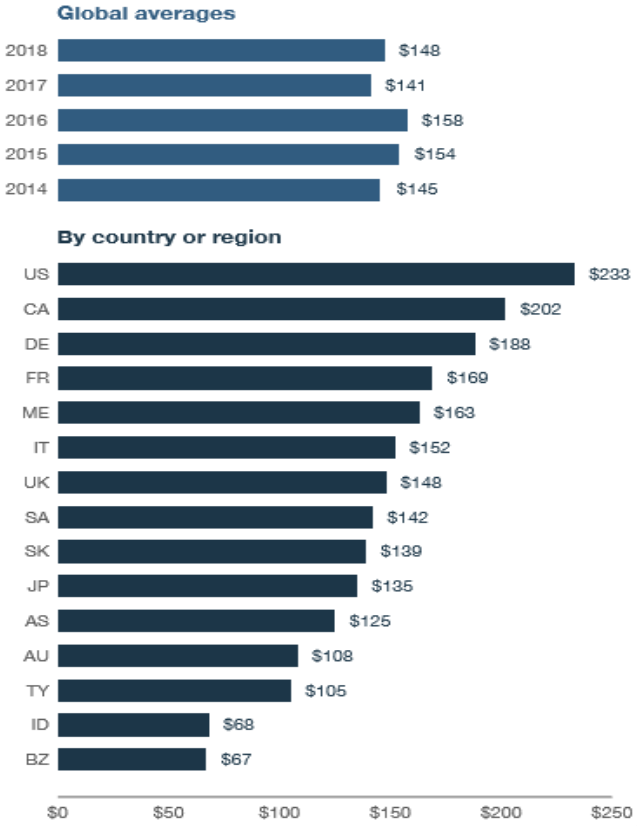
Non-compliance

Non-compliance Costs
Penalties and Fines oh my!

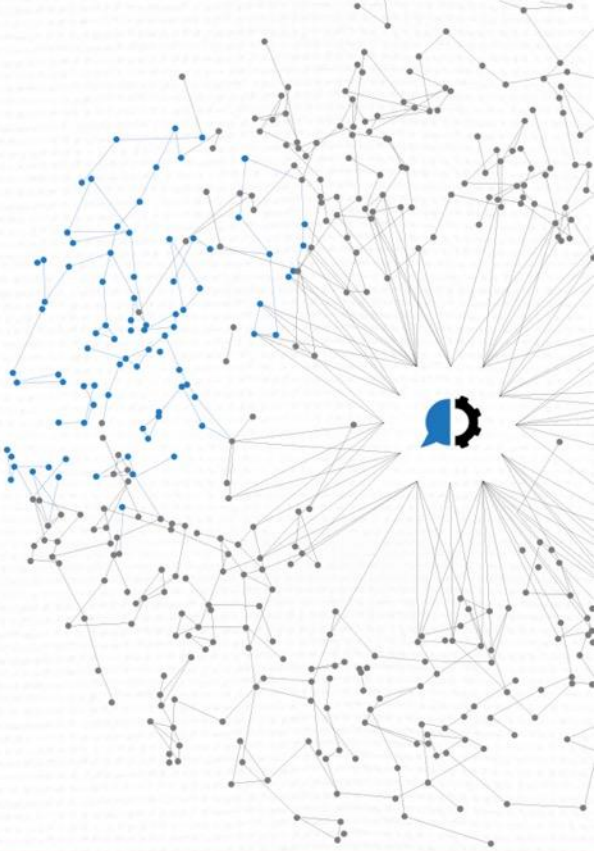
- PCI DSS
  - Up to $500,000 per incident
  - $50,000 per day
- GDPR
  - Up to 20 million Euro – approx. 22 million USD
  - Or 4% of worldwide annual revenue
  - Whichever is HIGHER
- HIPAA
  - Up to $50,000 per incident
  - Up to $1.5 million per year
  - Up to 10 years in jail
- FISMA
  - Loss of contract work
  - Federal funding cut
  - Censure by Congress

Non-compliance costs
Data Breach

- The consolidated average per capita cost for all samples was $148 compared to an average of $141 last year.
- The United States, Canada, and Germany continue to have the highest per capita costs at $233, $202, and $188, respectively.
- Turkey, India, and Brazil have much lower per capita costs at $105, $68, and $67, respectively.



Regulations and Laws



UP NEXT

HIPAA

- National set of security standards to protect health information – 1996 inception
- Protected Health Information
  - Individuals past/present/future physical or mental health condition
  - Provision of healthcare to individual
  - Past/present/future payment for provision of healthcare to individual
  - Individually identify someone
- HHS/OCR responsible for enforcement of Security Rule
- Purpose
  - CIA
  - Organizations be held accountable to protect patient data

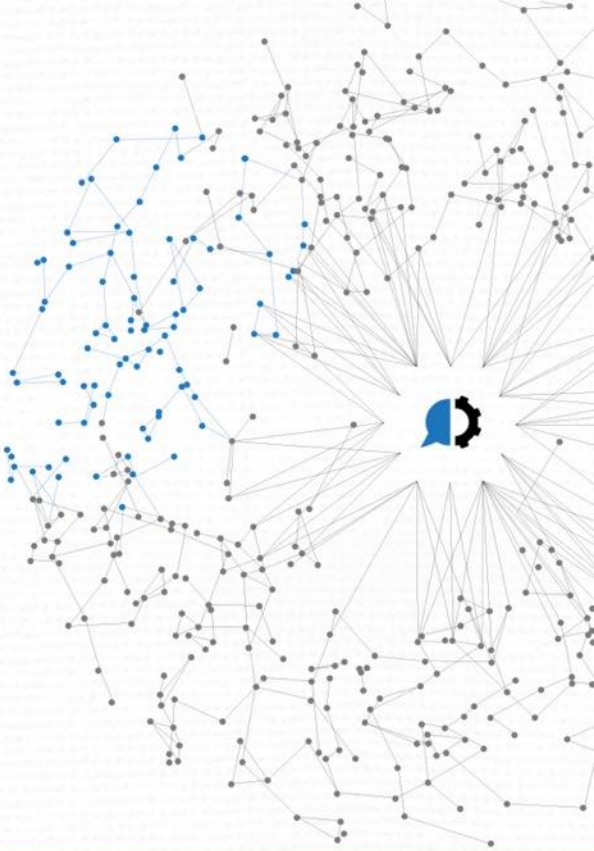
FISMA

- Federal Information Security Modernization Act (2014)
- National Instituted of Standards and Technology
  - Responsible for developing information security standards
  - Minimum requirements for Federal agencies
- Special Publications
  - Suite of documents outlining security guidelines
  - NIST 800-53r4
- FedRAMP
  - Federal Risk and Authorization Management Program
  - Not law
  - Framework or standardized approach to security for cloud deployments

GDPR

- General Data Protection Regulation
  - Enacted May of 2016
  - All businesses conducting operations in EU countries
  - All organizations process covered data for citizens in EU nations
- European Data Protection Board
  - Enforce regulations - https://edpb.europa.eu/news/national-news_en
  - DPA – Data Protection Authorities
  - DPA authority is quite extensive and can be subjective
- Fines can be quite large
  - $123 million for Marriott
  - $201 million for British Airways
- Purpose – to protect individual personal data and give users control of their own data (where stored, how used, power to delete, etc)

Standards



UP NEXT

ISO 27001 & 27002

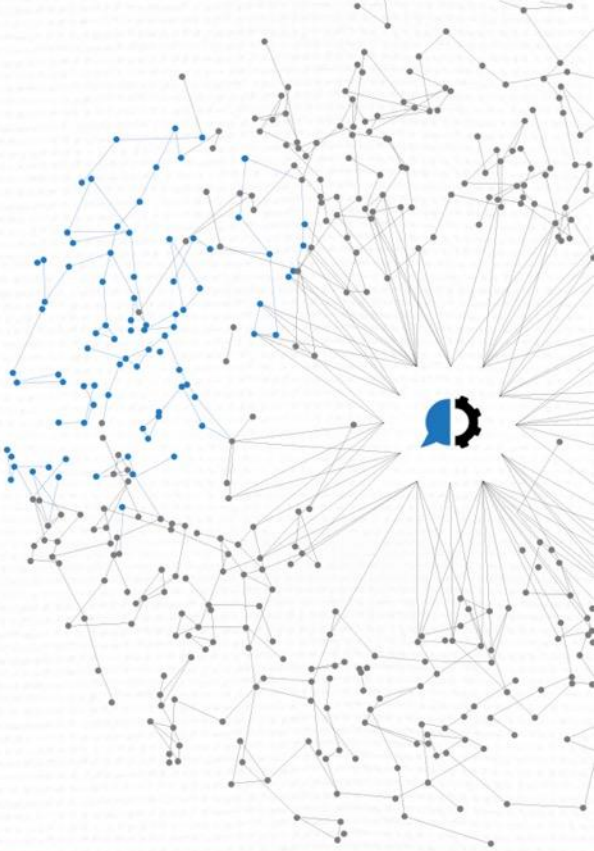
- International Organization for Standardization
  - Worldwide federation of national standard bodies
  - Standards carried out by technical committees
- ISO 27001
  - Provides normative requirements for information security management systems
  - Standard and not requirement for compliance
  - Organizations can require business partner or vendor to have ISO 27001 certification
  - Compliance can be certified by accreditation body
- ISO 27002
  - Security controls
    - 14 security control clauses
    - 35 main security categories
    - 114 specific controls
  - GoAnywhere actively pursuing ISO 27001 compliance

	2013	2014	2015	2016	2017
Total	21604	23005	27536	33290	39501
Growth Y2Y Total	10%	6%	20%	21%	19%

PCI - DSS

- Payment Card Industry Data Security Standard
  - Applies to ALL companies that accept, process, store or transmit CC information
  - PCI Security Standards Council created in September 2006
  - 4 merchant levels depending on size, amount of transactions and whether or not they have had a breach
  - Just released PCI 4.0 Nov 13, 2019
- Detailed outline of security controls
- Security Settings Audit Report
- Member of the Standards Council

Organizational Frameworks



UP NEXT

Compliance – Organizational Frameworks

- RMF – Risk Management Framework
  - National Institute of Standards and Technology
  - Special Publications – 800-53r4
- CIS – Center for Internet Security
  - Top 20 critical security controls
  - Basic, Foundational, Organizational
- COBIT 2019
  - Governance and Management Objectives
  - Developed by ISACA.org
- IRS Publication 1075
  - Mission to protect confidentiality of tax payers information
  - Protecting all Federal Tax Information (FTI)

Compliance – Organizational Frameworks

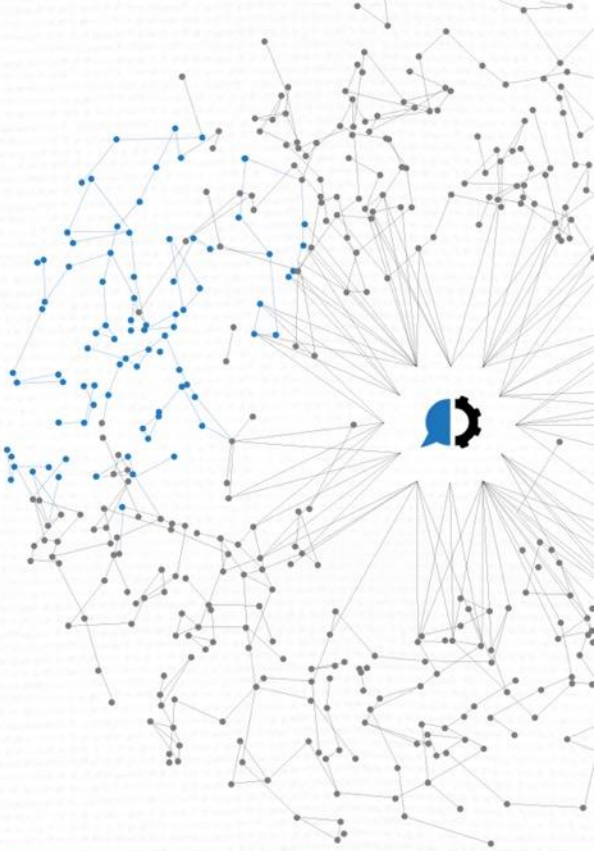
- Common Criteria
  - NIAP – National Information Assurance Program
  - CCEVS – Common Criteria Evaluation and Validation Scheme
    - Develop protection profiles, eval methodologies and policies
    - Evaluate COTS IT for conformance
- GoAnywhere actively pursuing 3 categories for certification
  - Protection Profile for Application Software
  - Functional Package for Transport Layer Security
  - Extended Package for Secure Shell
- GoAnywhere – what does this mean?
  - Strictly adheres to international standards
    - Encryption
    - Transmission of data
    - Secure transport sessions in accordance with the 3 aforementioned categories

What to do

- Know your industry
  - Identify any laws, regulations and or rules
  - Type of data
- Get C level buy in
- Pick your poison
  - Safeguards to address
  - Framework to use
- Tools to automate
- Tools to ensure appropriate protection
- Constant monitoring and evaluation

GoAnywhere Security

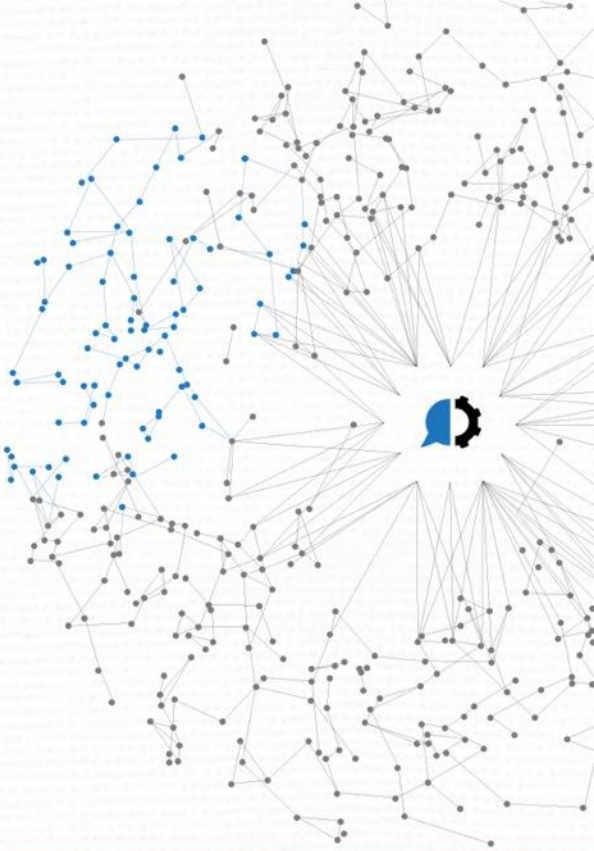
Demo



UP NEXT

helpsystems

Q&A



UP NEXT

helpsystems

Thank you for attending!

What next?

- https://www.goanywhere.com/resource-center/compliance
  - dan.freeman@helpsystems.com
  - www.goanywhere.com
  - Toll-free: 1-800-949-4696
  - Direct: 402-944-4242