Caught In The Dark Web

Presented By:

Ron Frechette
Founder & CEO

Sean Leinart
SOC Manager

PRESENTERS

Sean Leinart, Manager, Security & Support Services

sleinart@alertlogic.com

Sean serves as a Senior Manager in Alert Logic's Security Operations Center with over 20 years of experience in Information Technology with 10 years of that being directly related to Security. He has assisted several organizations with implementing their initial security infrastructures as well as serving as their Lead Security and Network Engineer. Most recently he leads a team of network security analysts for Alert Logic's ActiveWatch Enterprise Service offering.

PRESENTERS

Ron Frechette, Founder & CEO

ron.frechette@goldskysecurity.com

o: (407) 853 8404 c: (904) 610 3420

Ron serves as Chief Evangelist Officer for GoldSky Security with over 10 years of experience directing Security Risk Assessment engagements and developing Cybersecurity Plans for various size companies across North America. Known to many as “The Cyber Coach”, he is constantly studying emerging cybersecurity trends and shares his knowledge through blogging platforms, local publications and speaking engagements across various industries.

Ron’s area of expertise has evolved from supporting large enterprise companies to helping small-midsize businesses with their IT security and compliance needs. He has assisted various companies in becoming compliant with frameworks such as FedRAMP, FISMA, GLBA, HIPAA/HITECH, HITRUST CSF, ISO27001, NIST CSF, NIST 800-53, 800-171, NERC-CIP, PCI DSS, SSAE 18 (SOC1), SOC2 and SOC3.

AGENDA

- The World Wide Web
- The Dark Net
- The Threat Actors And Motivators
- Information Available & Impact
- Your Digital Footprint
- The Problem
- Cyber Security Adoption For SMBS
- Primary Objectives To Mitigate Risk
- A Cyber Risk Management System
- Practical Steps To Mitigate Your Risk
- Q&A

The World Wide Web

THE WORLD WIDE WEB

THE DARK NET

WHAT IS TOR

Tor is a service that helps you to protect your anonymity while using the Internet.

Developed in the mid-1990s by United States Naval Research Laboratory to protect US intelligence communications online.

Further developed by Defense Advanced Research Projects Agency (DARPA).

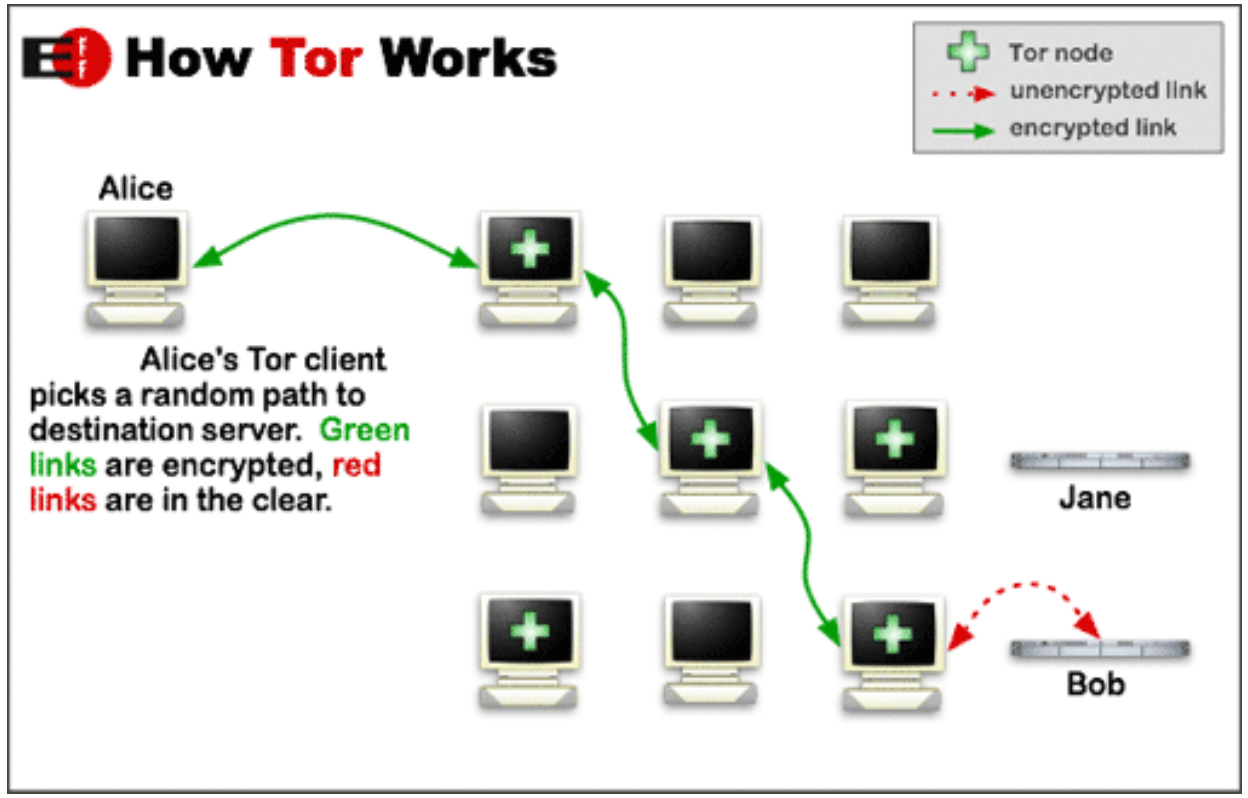
Tor is comprised of two parts:

- Software you can download that allows you to use the Internet anonymously,
- a volunteer network of computers that makes it possible for that software to work.

Source

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

HOW DOES IT WORK?



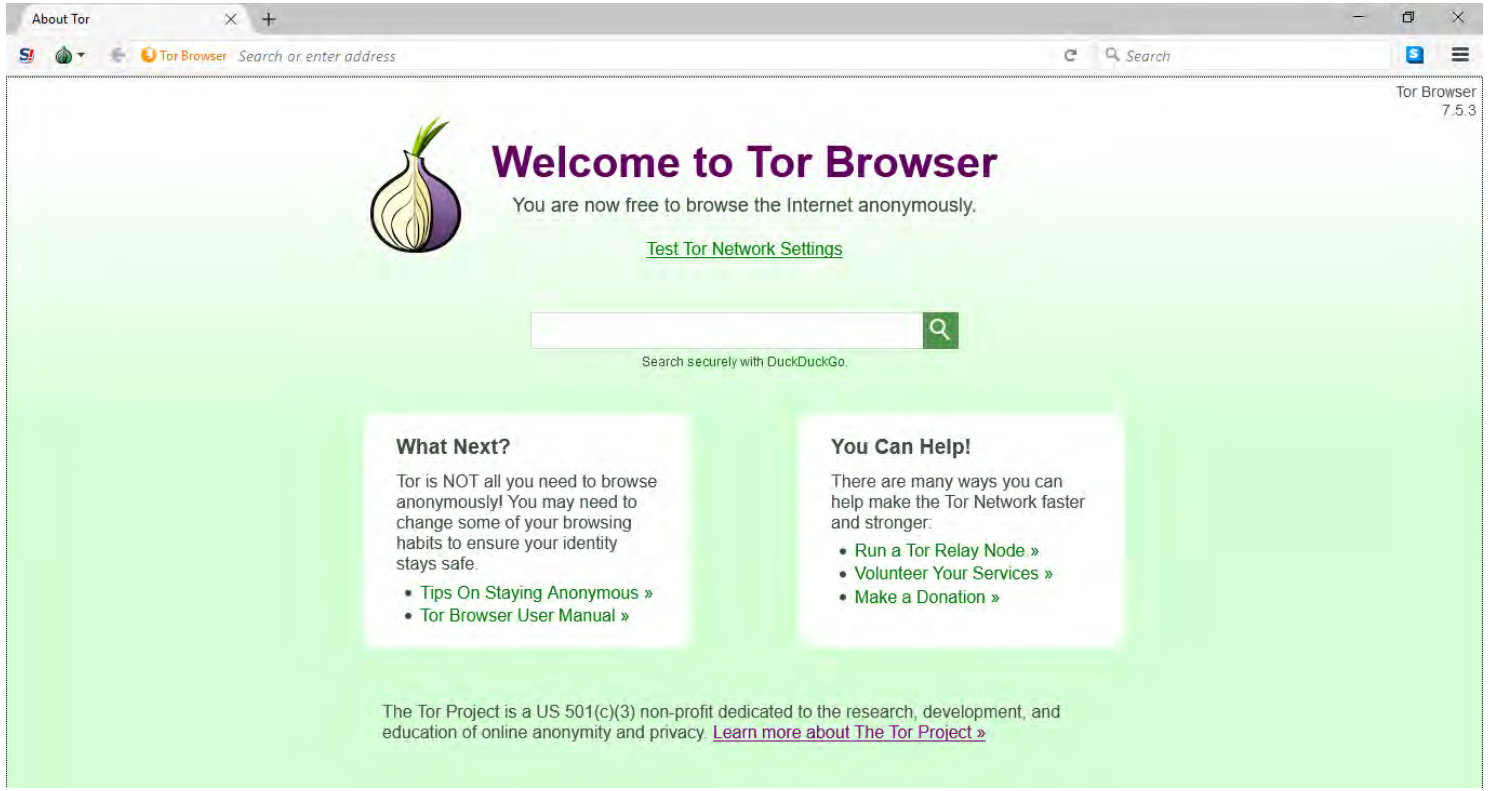
Encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe.

These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location

LIVE DEMO

ALERT LOGIC

Click To View Demo



The Threat
Actors & Motivators

WHO ARE THE ATTACKERS

Organized Crime Organizations
Large syndicates of attackers
Hierarchical organizations; Mafia

State-Sponsored Attackers
Governments
Russia, China, Iran, North Korea, etc...

Script Kiddies
Use downloaded tools and scripts
Motivated by fame and LULZ

Average Everyday Citizens
Revenge

Hacktivists
Collectives such as ANONYMOUS
Motivated by a social cause

WHAT'S THEIR MOTIVATION?

Organized Crime Organizations
Financially motivated
Control of criminal channels territories
Human trafficking

State-Sponsored Attackers
Cyberwarfare, spying, espionage

Script Kiddies
See what they can do and get away with
Entertainment and fame

Average Everyday Citizens
Scorned spouses
Cyberbullying
Drugs and other illegal activity

Hacktivists
Motivated by a social cause
Power in Numbers

Information Available & Impact

WHAT INFORMATION IS AVAILABLE?

Personal Information
Stolen credentials from subscribed services (Netflix, Disney+ etc…)
Social Security info, DMV info, Complete identities
Health records

Financial Information
Credit Card information
Bank Account information

Business Information
Stolen Information from hacking activity

Illegal Marketplaces (upwards of 50% or more of sites)
Drugs
Weapons
Illegal Services (hacking services)

Content
Pirated content (music, movies)
Video camera footage
Content gained from hacking activities (pictures, audio)

*** Make no assumption that there isn't some personal data about you on the Dark Web today*

WHAT'S THE IMPACT?

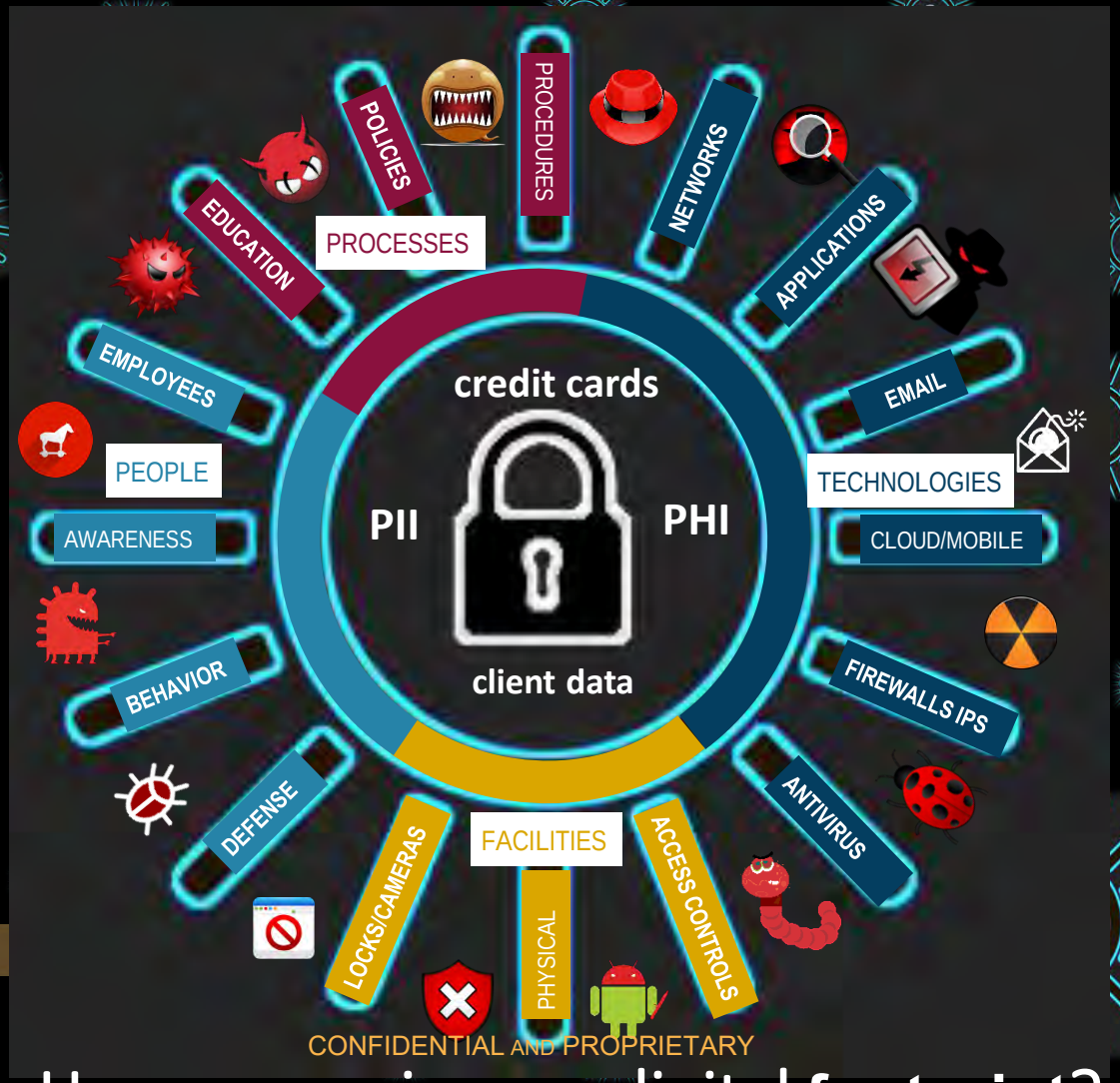
Personal
Complete identity stolen
Financial ruin
Damaged reputation

Business
Brand damage
Lawsuits
Fines
Time and Resources to recover from a breach

YOUR DIGITAL FOOTPRINT

YOUR DIGITAL FOOTPRINT

Four threat vectors around a digital footprint:



How secure is your digital **footprint**?

THE PROBLEM

WHAT'S THE PROBLEM?

Hackers are now targeting small-midsize businesses due to the sensitivity of data and lack of security measures deployed by a majority of SMBs.

Federal and State Compliance Regulators are beginning to enforce cybersecurity mandates on SMBs and imposing civil penalties due to increased number of cyber breaches.

Cybersecurity Awareness and Education is severely lacking in the SMB space, perceived to be hard to implement and expensive. Another common misperception is their IT managed service provider has them covered.

WHAT CAN YOU DO?

UNFORTUNATELY, NOT MUCH TODAY …

Ignore the problem and hope it goes away

OR PANIC …

Spend all the right money in all the wrong places

WHERE DO YOU FALL …

Nothing

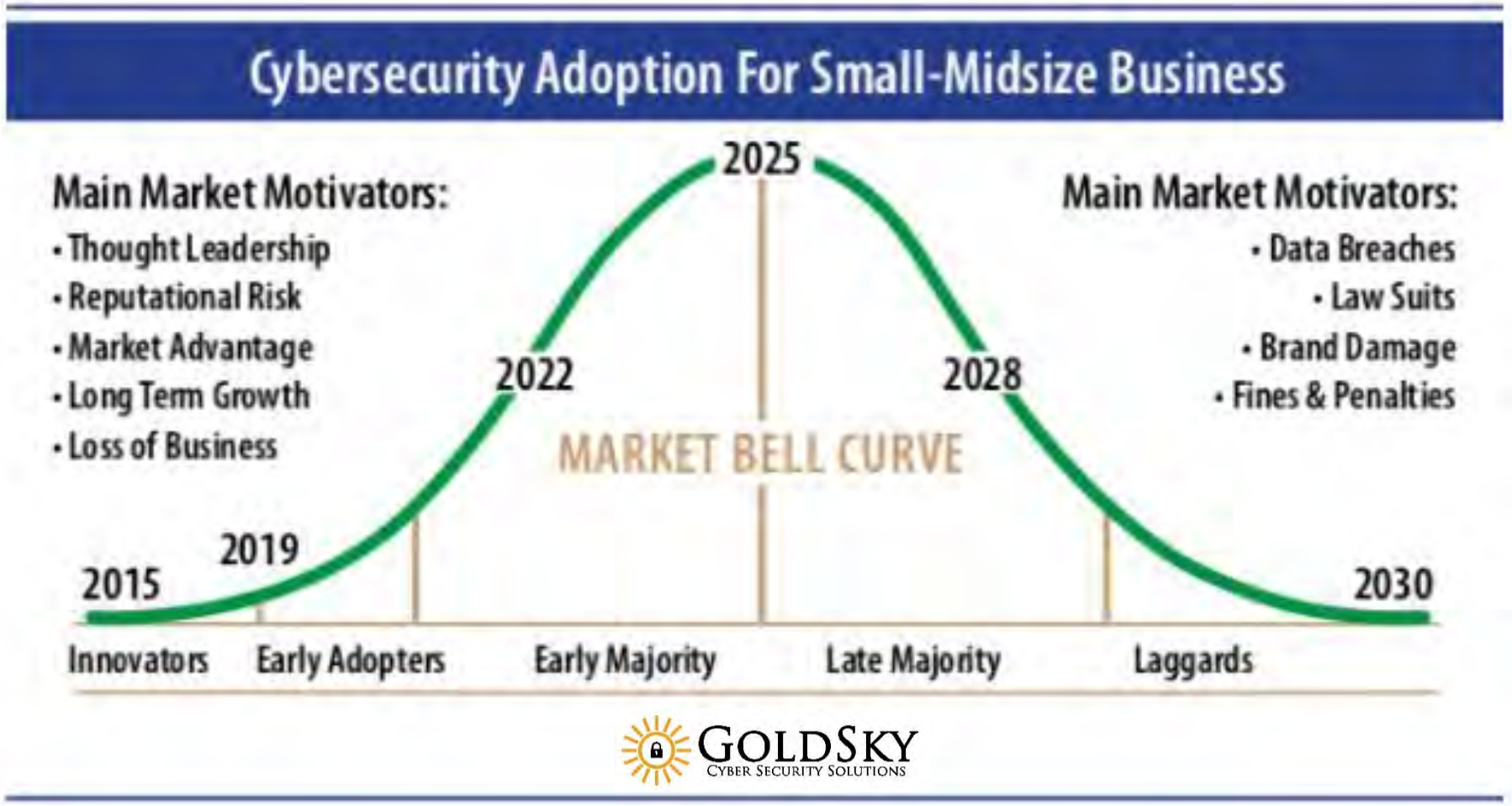
Ignore the problem and hope it goes away

Panic

Spend all the right money in all the wrong places

Cyber Security Adoption For SMB's

CYBERSECURITY ADOPTION FOR SMBs



Primary ObjectiveS To MitigatE Risk

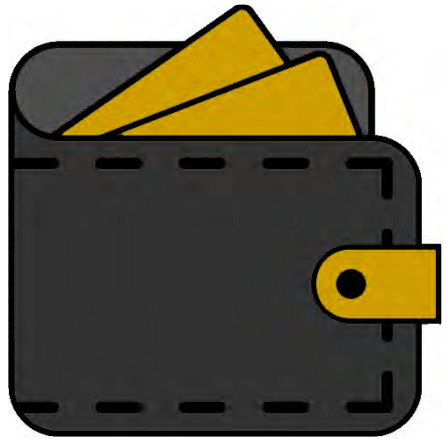
PRIMARY OBJECTIVES

Avoid Compromise

Costs and Brand Damage

Achieve Compliance

Follow the Law and Avoid Fines



Affordable Solutions

Custom Designed for SMBs

WHAT'S THE RIGHT APPROACH?

Evaluate, Identify, and Manage Risk

THE SECURITY RISK ASSESSMENT (SRA)

How we help our clients evaluate, identify, and manage risk…

National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP800-30 provides the Risk Assessment Methodology for all federal agencies to follow.

The private sector uses NIST as the foundation for all security controls and compliance frameworks in the US.

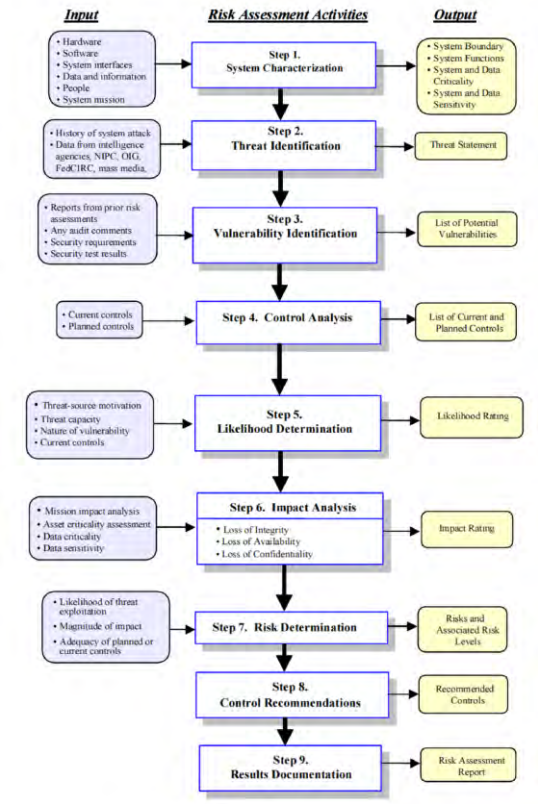


Figure 3-1. Risk Assessment Methodology Flowchart

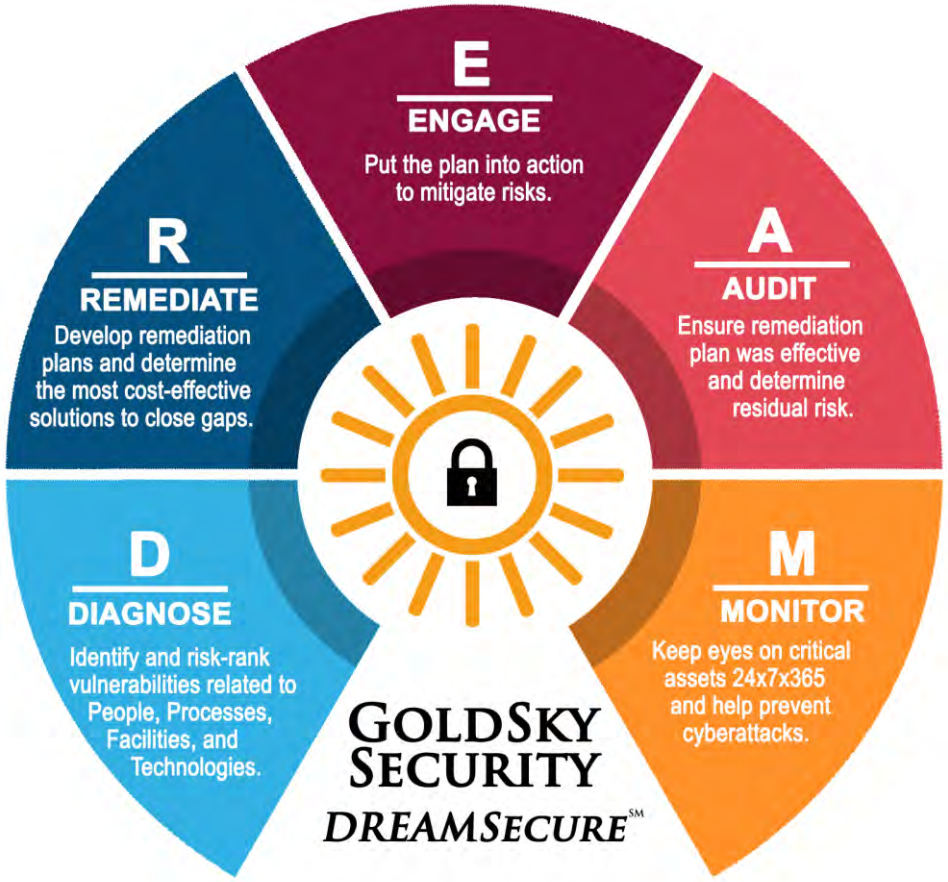
NIST BASED COMPLIANCE FRAMEWORKS

NIST SP800-53 rev.5 - provides a catalog of security controls for all U.S. federal information systems except those related to national security.

A CYBER RISK MANAGEMENT SYSTEM

ADOPTING A CYBER RISK MANAGEMENT SYSTEM

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



SAMPLE – SRA Letter of Completion

GOLDSKY
CYBER SECURITY SOLUTIONS

August 8, 2019

Michael Jones
Chief Information Officer
Healthcare Company, Inc.
85 GoldSky Lane, Suite 220
Orlando, FL 32801

RE: Completion of 2019 HIPAA Security Risk Analysis

Dear Michael,

This letter is to certify that GoldSky Security, LLC ("GoldSky") has completed a HIPAA Security Risk Analysis in accordance with US Code of Federal Regulations 45 CFR 164.308(a)(1) [HIPAA Security Rule, Administrative Safeguards, Security Management Process standard, Risk Analysis and Risk Management Implementation Specifications] and the HIPAA Breach Notification Rule 45 CFR 164.400-414.

It is evident Healthcare Company, Inc. is committed to the confidentiality, integrity, and availability of their client's data and services.

Sincerely,

Ron Frechette
Managing Partner
GoldSky Security, LLC

Atlanta | Boston | Denver | Nashville | Orlando | Phoenix | Tampa | Washington DC

PRACTICAL STEPS TO MITIGATE RISK

WHAT CAN YOU DO?

Personal

DO NOT REUSE PASSWORDS
Set a cadence to CHANGE your passwords
Use 2FA whenever possible
Leave no defaults on IoT or network devices
Practice least-privilege principal on personal devices
Use a monitoring service (there are paid and free)

Business

Practice a Defense-in-Depth approach to Security
Network Segmentation
Perimeter (firewalls, vpns)
IDS/IPS
AV/Endpoint
Log capture and retention
Patching and vulnerability management
(One size and one tool does not fit all)
Have an IR Plan (test it)
Good Backups and DR plans (test them)

Q&A

AND REMEMBER …

Thank you for your time and attention today!

THANK YOU!