



***Managing Risk and Improving Security –
Texas Cybersecurity Framework***

Jeremy Wolff, Joe Mancino
4/11/2017

NTT Security / Texas ISF

Agenda

NTT Security Background

Back to Basics

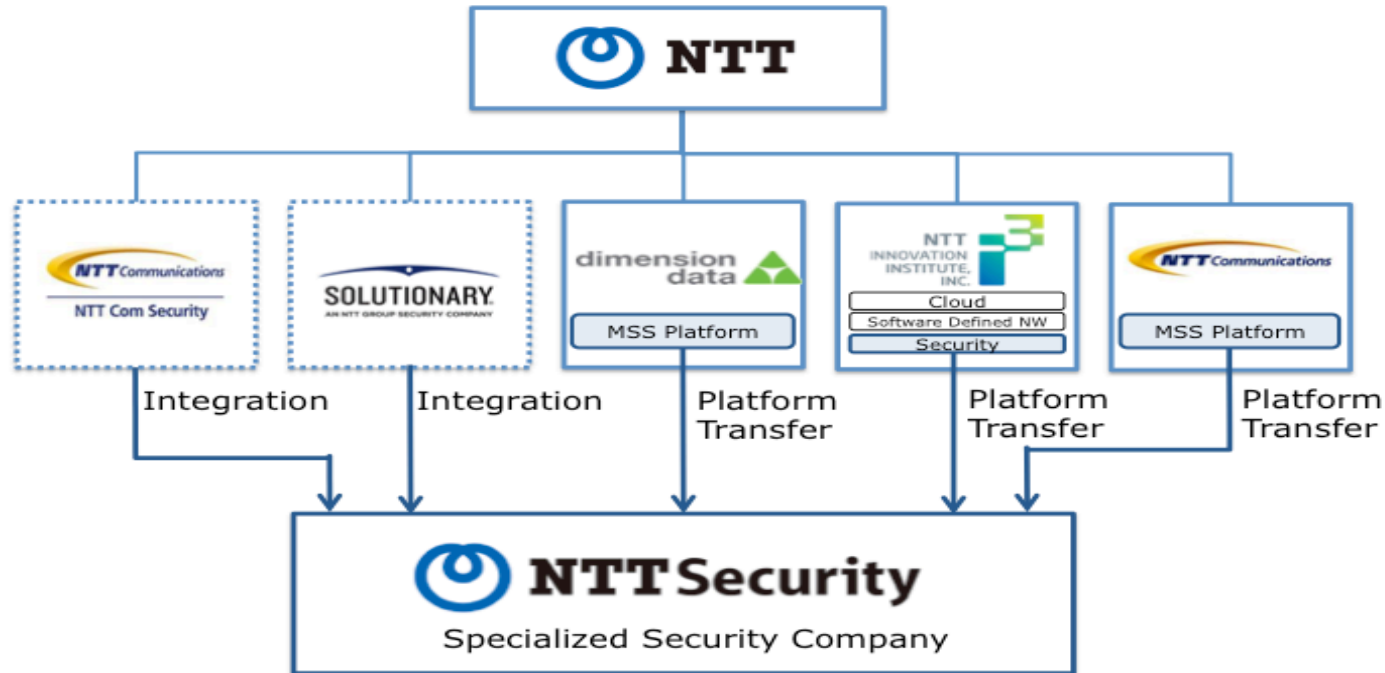
- Patching
- System Configuration
- Passwords
- Data Retention
- Encryption

Texas Cybersecurity Framework Assessments

Common Security Issues

Q&A

Formation of NTT Security - A specialized security company



NTT Security / NTT DATA – 2000+ Security Experts

Managed Security Services (MSS)

- 24/7 security analyst and proprietary advanced security information analysis platform enable real-time threat detection and validation, severity determination, reporting, remediation advisory and immediate isolation & protection.
- Additionally NTT Security provides secure IT lifecycle management with continuous vulnerability testing, patch management, advisory and compliance reporting.
- Managed Operations, Network, Endpoint, Identity, Incident Management, Asset, Threat Assessment

Professional Security Services (PSS)

- Technical support and advisories based on security specialized expertise that enables organization's security risk identification, implementation of the right controls, appropriate incident response and forensics.
- GRC, Architecture/Design, Deployment, Integration, Threat Services, Assessments, and Advisory Consulting

2016-2020 Texas State Strategic Plan for Information Resources Management

Strategic Goal 1: Reliable & Secure Services

Strategic Goal 2: Mature IT Resources Management

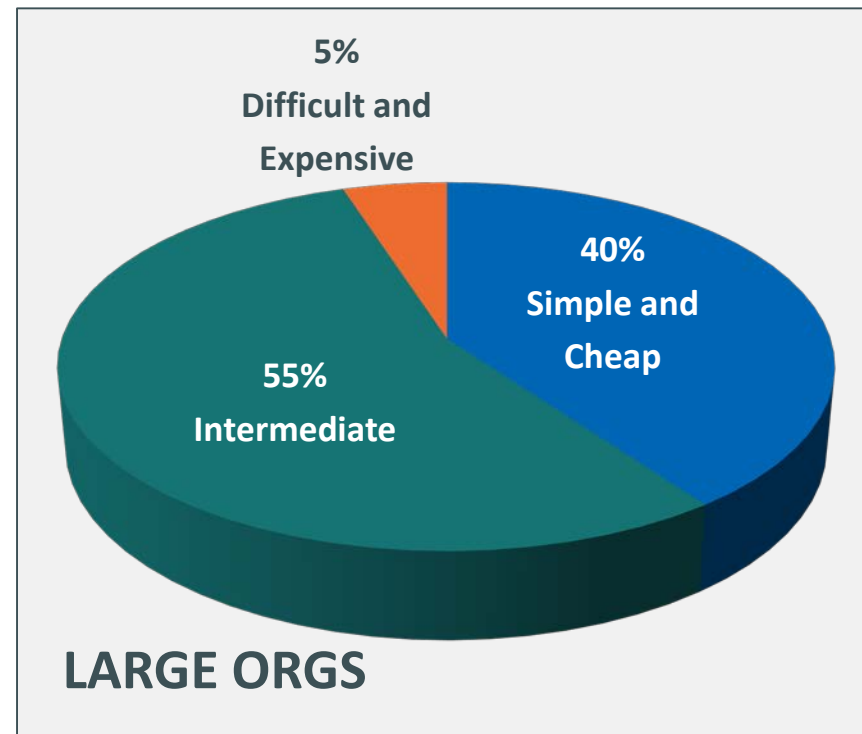
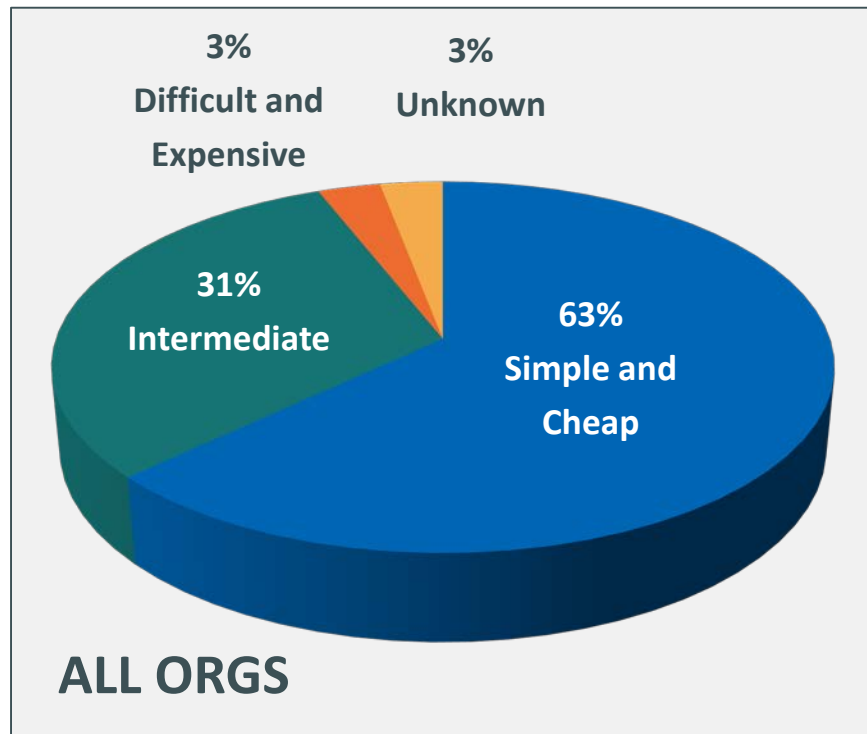
Strategic Goal 3: Cost-Effective & Collaborative Solutions

Strategic Goal 4: Data Utility

Strategic Goal 5: Mobile & Digital Services

Back to Basics

Difficulty of Breaching an Organization



Security Basics – Part 1

Patching	Chronically behind
	Legacy systems “can’t be patched”
System Configs	Default and insecure
	Infrastructure devices
Passwords	Blank, default, and weak
	Reuse

Security Basics – Part 2

Data
Retention

Storing unnecessary data

Storing data longer than necessary

Encryption

Using weak or no encryption

Not managing keys and certificates

Business as Usual

Formal processes

Patching

Hardening

Testing

Before deployment and in production

Base on industry standards (NIST, CIS, etc.)

Update process to address new vulnerabilities

Patching

50% of vulnerabilities identified in scan data for 2013 were first discovered between 2004 and 2011

Common Vulnerability Types

Information Leakage

- Attacker gets info that may lead to any of the conditions below

Denial of Service

- Nobody can use your system

Remote Code Execution

- Attacker gains control over your software

Privilege Escalation

- Attacker with low level access gains higher level access

Attack Vectors

Remote Exploit

- Vulnerable service exposed to Internet

Drive By

- Vulnerable client software opens malicious site or file

Local Exploit

- Exploit vulnerabilities not exposed to the network

Configurations

Through 2020, 99% of firewall breaches will be caused by misconfigurations, not security flaws. – Gartner research

Reduce the Attack Surface

Remove unnecessary software

Disable unnecessary services

Disable unnecessary backwards compatibility

Disable unnecessary features

Remove or change default accounts and credentials

Set all security options as tight as you can

Applies to operating system and
every piece of software on top of it

Passwords



76% of network intrusions exploited weak or stolen credentials. Strict policies are required to reduce this easily preventable risk.

Strong Password Policy

Enforce password requirements

Change
<90 days

12+
characters

All
character
types

Prohibit
re-use

Pattern
checks?

Support

Crack your own
passwords

Awareness of phishing
and re-use

When it really needs to be secure – multi-factor



Something You Know

PIN

Password



Something You Have

Token Card

Certificate File

Common Issues

Broken authentication and session management

Password reset procedures

Leaking plaintext passwords

Users with the same password on every site

Users who fall for phishing

Malware and keyloggers


Encryption

Many of the hacks that make the news can be attributed to weak or -- even worse -- nonexistent encryption. — Bruce Schneier

Untrusted Networks

Encrypt your data!

Or keep it out completely.



login	pass	domain ip	application
h00p	tde*****	65.154.34.164	HTTP
voltage*spike@fastmail.fm	tha*****	66.111.4.52	IMAP
Jennifer.lee@post.harvard.edu	pu*****	184.73.159.65	foursquare
denblew	MIC*****	137.52.224.216	pop
wencevdu	Sl*****	128.242.245.20	Twitter (on Android)
Nokia-asso-rx-49	JOS*****	207.114.197.94	HTTP
computicu	lof*****	128.242.245.116	Twitter
reuhelix	fay*****	128.242.245.116	Twitter
vishakn@yahoo.com	hea*****	184.73.159.65	foursquare
em2827891836	622*****	207.114.197.95	HTTP
rossknapp@gmail.com	863*****	184.73.159.65	foursquare
mylongs	tes*****	128.242.245.43	TWITTER
erissti	int*****	128.242.245.148	Twitter
6062191197	pre*****	184.73.159.65	foursquare
otkrisnan	4lj*****	128.242.245.20	twitter
	Co*****	184.73.159.65	4square

Anything that happens over radio (WiFi, Bluetooth, Cellular)

Any wire that leaves your building (Internet, MPLS, Point-to-point)

Any network with a workstation on it (Phishing targets)

Any network with public IP addresses on it (Zero days)

Application Security

Not basic perhaps, but fundamental to supporting the organization's mission.

Application Vulnerabilities



Injection

Cross Site Scripting

Broken Authentication and Session Management

Insecure Direct Object References

Cross Site Request Forgery

Security Misconfiguration

Insecure Cryptographic Storage

Failure to Restrict URL Access

Insufficient Transport Layer Protection

Unvalidated Redirects and Forwards

For more information

<http://www.owasp.org>

Software Development Lifecycle

Use Coding standards

- OWASP
- QA for security, not just functionality

Dev/test/prod/backup environments

- Change control
- No testing in production environment
- No production data in test environment

Treat the cause, not the symptom

- Proper design can prevent vulnerabilities
- Stored procedures, standardized libraries, centralized error handling

People

Users don't want to be insecure, they just don't know how not to be

- Where and what are the policies?
- Demonstrate real-world threats
- Initial and ongoing training
- The highest value targets often exempt themselves from the rules

Managing Risk and Improving Security –

Texas Cybersecurity Framework

Texas Cybersecurity Framework – 40 Security Control Categories

Privacy & Confidentiality	Physical and Environmental Protection
Data Classification	Personnel Security
Critical Information Asset Inventory	Third-Party Personnel Security
Enterprise Security Policy, Standards and Guidelines	System Configuration Hardening & Patch Management
Control Oversight and Safeguard Assurance	Access Control
Information Security Risk Management	Account Management
Security Oversight and Governance	Security Systems Management
Security Compliance and Regulatory Requirements Mgmt	Network Access and Perimeter Controls
Cloud Usage and Security	Internet Content Filtering
Security Assessment and Authorization/ Technology Risk Assessments	Data Loss Prevention
External Vendors and Third Party Providers	Identification & Authentication
Enterprise Architecture, Roadmap & Emerging Technology	Spam Filtering
Secure System Services, Acquisition and Development	Portable & Remote Computing
Security Awareness and Training	System Communications Protection
Privacy Awareness and Training	Vulnerability Assessment
Cryptography	Malware Protection
Secure Configuration Management	Security Monitoring and Event Analysis
Change Management	Cyber-Security Incident Response
Contingency Planning	Privacy Incident Response
Media	Disaster Recovery Procedures

TX CSF CMM Scoring – General

Maturity Levels

LEVEL 0: Non-Existent. There is no evidence of the organization meeting the objective.	LEVEL 1: Initial. The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	LEVEL 2: Repeatable. The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.	LEVEL 3: Defined. The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	LEVEL 4: Managed. The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.	LEVEL 5: Optimized. The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.
--	--	---	---	---	--

Control Objective Maturity Indicators



Common Security Issues

Policy & Procedure Documentation

Asset Management

Vulnerability & Risk Management

Compliance (HIPAA, PCI...)

Logging Strategy

System Development Lifecycle

Incident Response

Configuration Standards

Perimeter Security

Change Management

Data Loss Prevention

Q&A

Thank you

Joe Mancino

214-770-0162

Joseph.Mancino@nttdata.com

Jeremy Wolff

917-576-6139

Jeremy.Wolff@nttsecurity.com