A Recipe For Creating The Ultimate Security Backstop
Scott Alldridge

• Co-founder and President of the IT Process Institute (ITPI)

• CEO of IP Services – Launched in 2001, IP Services developed within a branch of a Fortune 500 integrator

• Key role in developing and providing managed services and security services since before managed services was a recognized market

• Pioneered building services in the US based on a proven practices framework - ITIL

• Advised some of the world’s top service providers on IT best practices and service deliverables
The problem with Information Security is **NOT** security.

Most security issues are symptomatic of:

- Integrity Drift
- Shortfalls in Configuration Management
- Change Control
Expectations of Content

90%+ of the content included in this PowerPoint has been presented to the following government agencies and industry consortiums without change or alteration resulting in active dialog, projects and/or consulting engagements at the highest level in our government.
The Importance of IT Compliance and Managed Security Services

Information Technology Compliance & Managed Security Services from IP Services have earned the exclusive Endorsement of The American Hospital Association.

“I am encouraged to see AHA’s support and endorsement of IP Services’ Managed Security Services. It’s IP Services’ Visible Ops methodology that brings operational best practices together with compliance and security, to enable critical infrastructure to identify and mitigate malicious activity.”

Richard Marshall, Former Director of Global Cyber Security Management, Department of Homeland Security
The Importance of IT Compliance and Managed Security Services

“No longer is it feasible or economical for majority of our state banking association members to internally operate security solutions that can effectively and efficiently keep up with the demand and constant change of the IT threat landscape. IP Services has demonstrated a unique knowledge and IT management methodology that has proven security and compliance results.”

Gene Meyer, President of Synergy by Association

Synergy by Association is in partnership with over 40 state banking associations that represent more than 5,000 banks.
IT Process Institute Mission

To classify and study top performing IT organizations and identify the practices that make them both high performers operationally and more secure, and share those findings with those looking to improve IT within their organizations.

The ITPI engages in three primary activities:
- Research
- Benchmarking
- Prescriptive Guidance

Established over 14 years ago the ITPI is funded through sponsorship, research grants, and literature sales.

We exist to support the IT audit, security, and operations professionals.
ITPI Approach - Quantitative Decisions
Managing by FACT Not BELIEF

Research:
The Institute of Internal Auditors Research Foundation commissioned ITPI to conduct a study of how information technology controls impact operational performance and security.

Benchmarking:
Surveys and interviews were done by 850 executives from North American-based IT organizations. 15 performance measures and the use and maturity of 53 IT controls were analyzed to reveal key findings.

Prescriptive Guidance:
Visible Ops methodology was created as a result to simplify terminology and implementation of an ITIL framework where an ROI was most impactful.
Many breaches were discovered months, or even years after they occurred, all the while hackers were accessing sensitive data and personal information.

Some were only discovered after critical data and systems were locked down and inaccessible, bringing the daily operations to a complete halt.

Unauthorized access granted unknowingly by internal users through various social media or malware attacks, circumventing traditional security measures.
Security Spending vs Incidents

Traditional approach to solving the security problem continues falling short...something has to change

Security Spending in US

Compound Annual Growth Rate = 6.97%

Security Incidents (US Gov't agencies)

Compound Annual Growth Rate = 30.22%

Source: Telecommunications Industry Association, Wilkofsky Gruen Associates

Source: GAO-16-885T Page 2
Closing the Security Gaps

The gaps that will always exist "between" security point solutions can only be addressed with a comprehensive set of security controls that govern the way work is performed by staff and end users.

If those aspects of security aren't controlled effectively, the organization will be vulnerable to security breaches regardless of the amount of money spent on point-based solutions.

- Security isn't a "feature" that can be "bolted on" to IT work to compensate for an underlying insecure environment.
- In fact, spending more money on point-based security solutions may give organizations a false sense of security.
- If your core IT control processes are broken, that's a good indicator that your security is broken too.
- Security is a quality that must be addressed in every aspect of IT in order to achieve the desired results.
So Why Is Security Still A Problem?

The definition of insanity is doing the same thing over and over again, but expecting different results— Albert Einstein

Security incidents on average are outpacing security spending by a factor of 4:1

- Industry is still enamored with a bunch of point solutions
- Implementing point based solutions will always have gaps
- 50% of the 180 Enterprise IT leaders who responded to ComputerWorld’s recent poll said they will invest more next year in access control, intrusion prevention, identity management, and virus and malware protection.

Security Spending in US – CAGR is 6.97%

Security Incidents in US – CAGR is 30.22%
What is the Antidote?
So Many Best Practices & Security Frame Works


- Where do I start and why? Does one return more value than another?

- Information Technology Infrastructure Library (ITIL) premise:
  - IT plays a critical role in support of the business goals and requirements; security is not separated from this
  - Provides essential services to the organization supporting the business
  - Promotes quality and efficiency in the use of Information Technology & Security
  - Focuses on IT Service Management - IT Service Support and IT Service Delivery
The ITPI and ITIL

A big problem in the IT industry is that best practice frameworks and most advisory services aren’t based on **factual data**. ITPI’s 14+ years of research and data analysis uncovered three common ITIL service descriptions that lead to high performance/availability and highly secure IT services.

1. Release Management
2. Configuration Management
3. Change Management

20% of the ITIL focus nets 80% of the value

Focus on these three alone resulted in a tremendous IT service delivery **ROI** which became the basis for the Visible Ops Handbooks on how to practically implement an ITIL strategy.
The Visible Ops Handbook was the byproduct of the ITPI research and benchmarking to establish a methodology for gaining better control of IT environments through development of more effective Change Management, Configuration Management, and Release Management.

Visible Ops harmonizes its terminology and processes with the ITIL framework as a recipe for jumpstarting an ITIL initiative.
Benchmarking

ITPI analyzed the data including 57 individual practices and 15 performance measures, and identified 12 sets of practices commonly implemented together.

Seven of those sets of practices were shown to be statistically significant predictors of top levels of performance across the organizations in the study.

1. Release scheduling and rollback
2. Process culture
3. Pre-release testing
4. Standardized configuration strategy
5. Change linkage
6. Controlled production access
7. Process exception management
Benchmarking

*Nine controls* predict *60 percent* of the performance variation of organizations.
What Are Those Controls?

1. A defined process to analyze and diagnose the root cause of problems.
2. Providing IT personnel with accurate information about the current configuration.
3. Changes are thoroughly tested before release.
4. Well-defined roles and responsibilities for IT personnel.
5. A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents.
6. A defined process to identify consequences if service-level targets are not met.
7. A defined process for IT configuration management.
8. A defined process for testing releases before moving to the production environment.
9. A configuration management database describes the relationships and dependencies between configuration items (infrastructure components).
The Performance Results

Study participants were segmented based on their overall performance score as indicated by how many of the performance measures they scored in the top 50\textsuperscript{th} percentile of all survey respondents.

Highlights of the striking performance differentials for top-performers include:

- **Downtime minutes per month** - Top-performers average 30 minutes
- **Release impact rate** - Top-performers have an average 2.9\% of releases that cause a service outage or incident
- **Incidents fixed within SLA limits** - Top-performers fix 93\% of incidents within service level agreement (SLA) limits
- **Security breaches automatically detected** - Top-performers *auto-detect an average of 91\% of security breaches*
Quality Matters

The quantitative data proves that organizations that care about quality in IT are “top-performers” in their metrics. It is no accident they also achieve a much higher security standard and posture.

Why? Because they have:

1. A system for managing releases and configurations so they know they are in a solid, tested, and approved working state.
2. An effective Change Management system designed to mitigate configuration drift.
3. Included security in all IT activities, including configuration, change, and release processes.
4. Employed Continual Improvement process to ensure all organizational and security requirements are being met.
Integrity Has Been The Missing Ingredient

**Integrity**
Data integrity is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

**Security**
Computer Security is the process of preventing and detecting unauthorized use of your computer. It involves the process of safeguarding against intruders from using your computer resources for malicious intents or for their own gains (or even gaining access to them accidentally).

**Trusted Computing**
Trusted Computing ensures that a computer will consistently behave in expected ways, and those behaviors will be enforced by computer hardware and software.

Without **Integrity** you don’t have **Security**

Without **Security** you don’t have **Trusted Computing**
A New Security Paradigm

All security issues start with a CHANGE or NEED for CHANGE

- Incorporating Integrity Verification is essential to delivering Compliance & Security Service
- Known, authorized and expected configurations is paramount to operating a secure and trusted infrastructure
- Identification of change – Lower Mean Time To Detect (MTTD) needs to become the new norm
- Event Correlation that includes:
  - Security Incident and Event Management (SIEM)
  - File and System Integrity Management (FSIM)
- Couple the ITPI benchmark results of an auto-detect average of 91% of security breaches with Event Correlation, an organization can truly achieve Trusted Computing
Next Generation CyberSecurity

• Focusing on managing changes and configurations, coupled with integrity verification will create the ultimate security backstop.

• As a result of implementing Next Generation CyberSecurity customers will:
  – Move from the industry average of mean time to detect from 191 days to 1 day
  – Provided prompt reporting on change and management of the key infrastructure metrics
  – Demonstrate IT compliance on a daily basis
  – Reduce IT costs 20% on average and increase monthly uptime
  – Increase operational efficiency and customer satisfaction – and other benefits
Managed Security Services - IP Services Offers

Core Service Foundation
Managed Integrity as a Service (MIaaS)

Best of Breed Point Solutions

- BYOD Security
- Endpoint Security
- Vulnerability Assessment
- Encryption
- DDoS Mitigation
- Audit Compliance
- Firewall Management
- Identity and Access Management
- Penetration Testing
- Intrusion Prevention Systems
- Mail Security
- Virtual Private Network Management
- Security Awareness Training
- Web Application Firewalls
- Security Policy and Compliance Consulting
As A Result – Implementing The Discussed Solution

16 years of experience has driven the following results:

– The endorsed CyberSecurity Suite of services has achieve some of the highest levels of *security performance* the industry has ever seen.

– Provided *prompt reporting* and management of the key infrastructure metrics.

– Ability to *demonstrate IT compliance* on a daily basis.

– Customers have reduced IT costs on average of 20 percent per customer and achieved monthly *uptime of 99.99 percent* on average.

– Increased operational efficiency and customer satisfaction due to *increased service levels*. 
Summary

As organizations develop security and compliance measures that take into account HIPPA, FFIEC, PCI and other regulatory bodies, they need a compliance and security strategy that will include:

• An IT management methodology that includes change, configuration and release management as a core component to an effective security strategy – this is better known as Visible Ops

• Event Correlation with SIEM and FSIM
  – Vulnerability assessment and baselining
  – Risk analysis, security alerts and system activity reporting
  – Continuous compliance reporting

• Delivered as a cost effective managed security service
Keep in mind...

A FOOL with a TOOL is still a FOOL...to avoid this you must:

• Focus on the right things, is your IT organization following best practices and processes such as ITIL?

• Will they be able to achieve and maintain the appropriate IT Controls and IT Service quality required to ensure a strong security posture and risk mitigation capabilities?

• Employ the appropriate Integrity Verification, Event Correlation, Detective Controls to give your organization the ULTIMATE SECURITY BACKSTOP!