WITHOUT SYSTEMS INTEGRITY YOU DON'T HAVE SECURITY AND YOU DON'T HAVE TRUSTED COMPUTING

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) starting in 2002
- Advised some of the world's top service providers on IT best practices and service deliverables

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

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

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

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

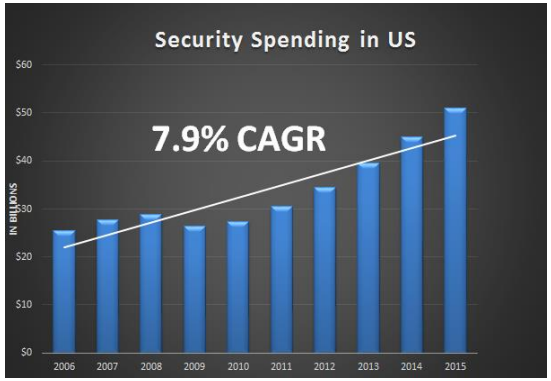
Prescriptive Guidance:
Visible Ops methodology was created as a result to simplify terminology and implementation of an ITIL framework where an ROI was most impactful

Unknown Security Risks & Time Bombs

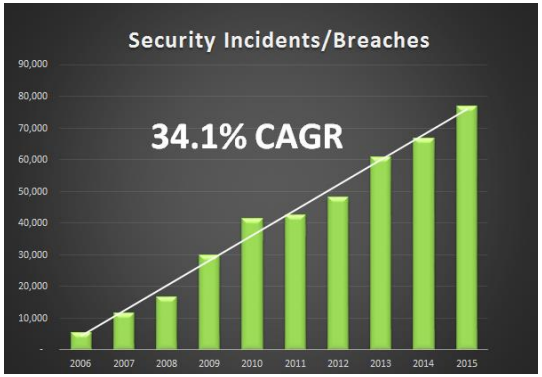
- Many breaches were discovered months, or even years after they occurred, all the while hackers were accessing sensitive data and personal information.
- Some were only discovered after critical data and systems were locked down and inaccessible, bringing the daily operations to a complete halt.
- Unauthorized access granted unknowingly by internal users through various social media or malware attacks, circumventing traditional security measures.

We Know The Security Market Has A Problem!

The Security Industry Is Broken…Something Has To Change!



Source: Telecommunications Industry Association, Wilkofsky Gruen Associates



Source: Government Accountability Office

Very Apparent We Can Not Spend Your Way Out Of Security Problems!

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

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 Spending in US – CAGR is 7.9%

Security Incidents in US – CAGR is 34.1%

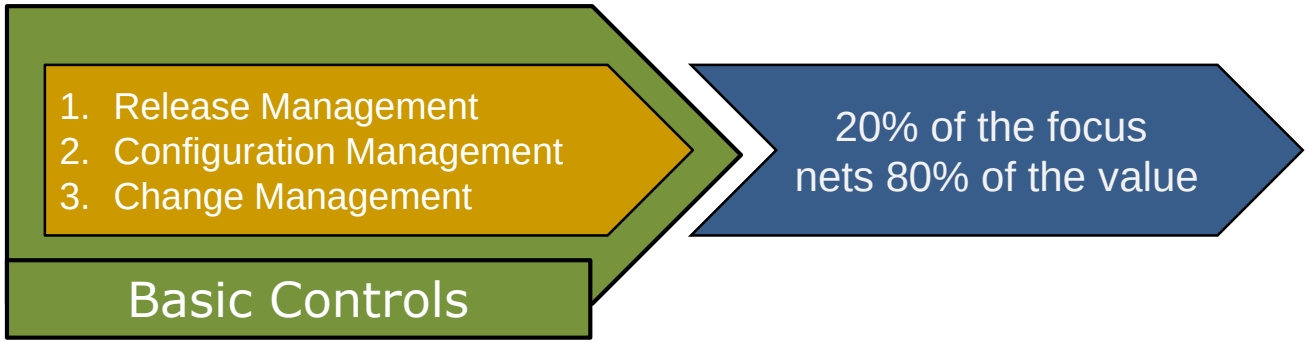
Security incidents on average are outpacing security spending by a factor of 4:1

- 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.

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

Where To Start…

A big problem in the IT industry is that best practice frameworks and most advisory services are not based on ***factual data***. ITPI's 14+ years of research, data analysis and benchmarking over 850 organizations uncovered **three common service descriptions** that lead to highly secure IT services.



IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

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.

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

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).

A Critical Performance Conclusion

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

One unique example of a result highlighted by the top-performers indicated that ***91% of all security breaches were auto-detected*** when **release**, **change** and **configuration management controls** were implemented.

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

So is the CyberSecurity answer your SOC or NOC?

So one of the most common/popular approaches to managing security is deploying, improving, or outsourcing a SOC or NOC. However, this can leave HUGE GAPS.

However, satisfaction numbers dip below 50% for SOC-NOC (network operations center) coordination and effectiveness, as well as the ability to detect previously unknown threats, which is also the capability that received the most "not satisfied" responses, at 45%. These are clear areas where more automation and integration will help organizations take their SOCs to the next level.

Security operations centers (SOCs) are growing up, according to a new SANS survey. Respondents indicated that the SOC's primary strengths are flexibility and adaptability while its biggest weakness is lack of visibility:

- SOCs still can't detect previously unknown threats, which is a consistent problem across many other SANS surveys.
- The survey indicates a willingness to integrate the prevention, detection and response functions – particularly in prevention and detection, where the tools respondents use are mostly the same.

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

NOC/SOC - Continued

- The SOC is a new and developing space architected in many ways across organizations with some consensus on what should be done: log, monitor, correlate and respond. The notion of an incident seems to be clear in the SOC, yet performance assessment capability and alignment to business appears lacking and is an important area for improvement.
- The survey highlights that a lot of SOC data collection and analysis is done via manual methods, meaning the need to sift through and correlate hundreds of events every day. Automation of data collection and analysis can empower SOC teams to deal with the overwhelming number of alerts with confidence.
- Results also show that many organizations are moving some portion of their SOC to managed service providers. This model seeks efficiency by transferring tasks to a third party, but it risks diminishing the tailored actions and localized knowledge associated with the needs of the business.
- The use of clearly articulated metrics to express performance offers an opportunity to improve SOCs. Development of useful metrics requires reuse of available data and selection of performance criteria that are valuable to the specific business needs and measure the effectiveness of the SOCs detection and remediation activities. Metrics are challenging, however, because there's not always a consensus on what makes good metrics within the SOC.
- Another opportunity for enhancement is more effective collaboration between NOCs and SOCs. Organizations have been performing IT operations for a long time, while SOCs typically are newer phenomena. The SOC and NOC can share data access to help IT operations make effective architecture decisions and to help the SOC make effective containment and monitoring decisions. Hunting and correlation are other areas organizations should improve on over the next 24 months.
- The alchemical formula for completely effective SOCs won't be cracked in the immediate future. But over the course of the next year, we will likely see a better community consensus of what a SOC is.

Source - Future SOC: SANS 2017
Security Operations Center Survey

Stop Being Enamored By Shiny Objects!

Continuous Integrity Management that includes configuration and change management at its core is what drives security.

YES…it's your core IT processes!

NOT…more SOCs, NOCs, CSIRT/CERT teams, SIEM tools, firewalls/IPS/IDS, threat intelligence solutions/artificial intelligence, or whatever shiny toy a company's security leadership or team decides is amazing and cool. Certainly these are all important elements of a holistic approach to managing CyberSecurity Risks, but not the end-all, be-all!

This is what the quantitative science continues to prove time and time again!"

Is There A Difference Between Change Management and Change Control?

Change Management is blind. It's a key IT Service Management process and most would agree that its beneficial to plan and schedule changes. But Change Management's 'dirty little secret' is that there is never any awareness of what's really going on. You simply don't know what was actually changed, either during the Change Window or at any other time.

Why does that matter? First, you don't know if changes you wanted were correctly implemented, in spite of all that planning. And from a security standpoint, you have no way of knowing the difference between everyday IT activity and a stealthy cyber-attack. It's precisely why, according to the 2018 Verizon Data Breach Investigation Report, 68% of breaches took months to discover.

Change Control solves these key problems by providing complete visibility of all changes.

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

So…IT Process Institute Asserts The Following

The problem with Information Security is **NOT** security.

Most security issues are symptomatic of:

Integrity Drift and shortfalls in Configuration Management and Change Control

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

So Why Hasn't The Analysts Defined An Integrity Management Market?

- Leading analyst firms are for profit and are driven by a "pay to play" scenario
- Many feel the analyst firms really do not want to solve the problem…it would result in a drastic decline in revenue
- The security market is and has been driven by bright shiny objects and the pursuit of silver bullets
- Integrity Management is not sexy…requires a knowledge of best practices of basic IT management principals
- Security and Operations still continue to operate independently from one another
- One vendor had a foothold on "Integrity" but has lost strategic vision and thought leadership over the past decade
- Until now…technology companies could not find a way to solve the problem of change noise (amount and velocity)
- SIEM vendors continue to misrepresent and confuse "Integrity Management" with "File Integrity Management"

SANS Understands…Integrity *IS* Foundational?

"IT Security is the process of implementing measures and systems designed to securely protect and safeguard information (…) against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure (…)"

Integrity Management can further be defined to include the following basic controls:

- Asset Mgmt
- Configuration Mgmt
- Change Mgmt
- Vulnerability Mgmt

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

Does The ITPI Data Support The Basic Controls

If we trust the data that says ***nine controls*** predict 60% of IT performance and ***91%*** of all security events can be auto-detected by way of proper ***release***, ***change*** and ***configuration management*** solutions…what are those priorities?

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

Foundational CIS Controls

ITPI Verified

ITPI Verified

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

ITPI Verified

15 Wireless Access Control

16 Account Monitoring and Control

ITPI Verified

Organizational CIS Controls

ITPI Verified

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

IT PROCESS INSTITUTE

RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

Much of IT Leadership is misguided and in large part NOT Managing by Fact

So contrary to the facts and focusing on process improvements, and developing a culture of causality, the "group think" of IT leaders by large percentage is represented in this recent survey;

"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"

So when engaging folks in IT Leadership (IT Directors, Managers); even with CTO & CIO folks this starts to be come the indicator there may be a problem in IT leadership!

Prescriptive Guidance

IT Process Institute wrote the book on it!

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 terminology and processes with another leading framework called ITIL. The Visible Ops Handbook series has sold over 400,000 copies.

IT PROCESS INSTITUTE
RESEARCH | BENCHMARKING | PRESCRIPTIVE GUIDANCE

Keep in mind…

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

- Be able to select the appropriate and necessary controls that align with the business strategy while mitigating risk and security threats
- Focus on the right things…is your IT organization following IT best practices and processes?
- Leverage proven foundational controls and best practices (i.e. SANS Critical Security Controls, VisibleOps methodology, etc…) to avoid recreating the wheel
- Be able to deploy and maintain the necessary controls to ensure proper operation and delivery

Leveraging IP Services As A Trusted Partner

17 years of experience has driven the following results:

- Increased operational efficiency and customer satisfaction due to ***increased service levels*****.**
- The highest levels of ***security performance*** the industry has ever seen.
- ***Prompt reporting*** and management of the key infrastructure metrics.
- Ability to ***demonstrate IT compliance*** on a daily basis.
- High Availability, with monthly ***uptime of 99.99 percent*** on average.
- All delivered as a ***cost effective*** managed services/security services

IP SERVICES

Scott Alldridge

IT Process Institute

scott.alldridge@ipservices.com

scott.alldridge@itpi.org

What is the Antidote?

So Many Best Practices & Security Frame Works

SANS Critical Security Controls – NIST Cybersecurity Framework – ITIL - PCI Data Security Standard - HIPAA - COBIT - ISO 27001/27002 – HITRUST - COSO Enterprise Risk Management – CMMI – LEAN IT – FFIEC - And many more…

- Where do I start and why?
- Does one return more value than another?
- Which one(s) are mandated by the government and who must comply?
- How do I provide verification that I am compliant?
- Is there any commonality between these frameworks?