DefenseNews

A GANNETT COMPANY

Shut Down the Hackers

Presented with

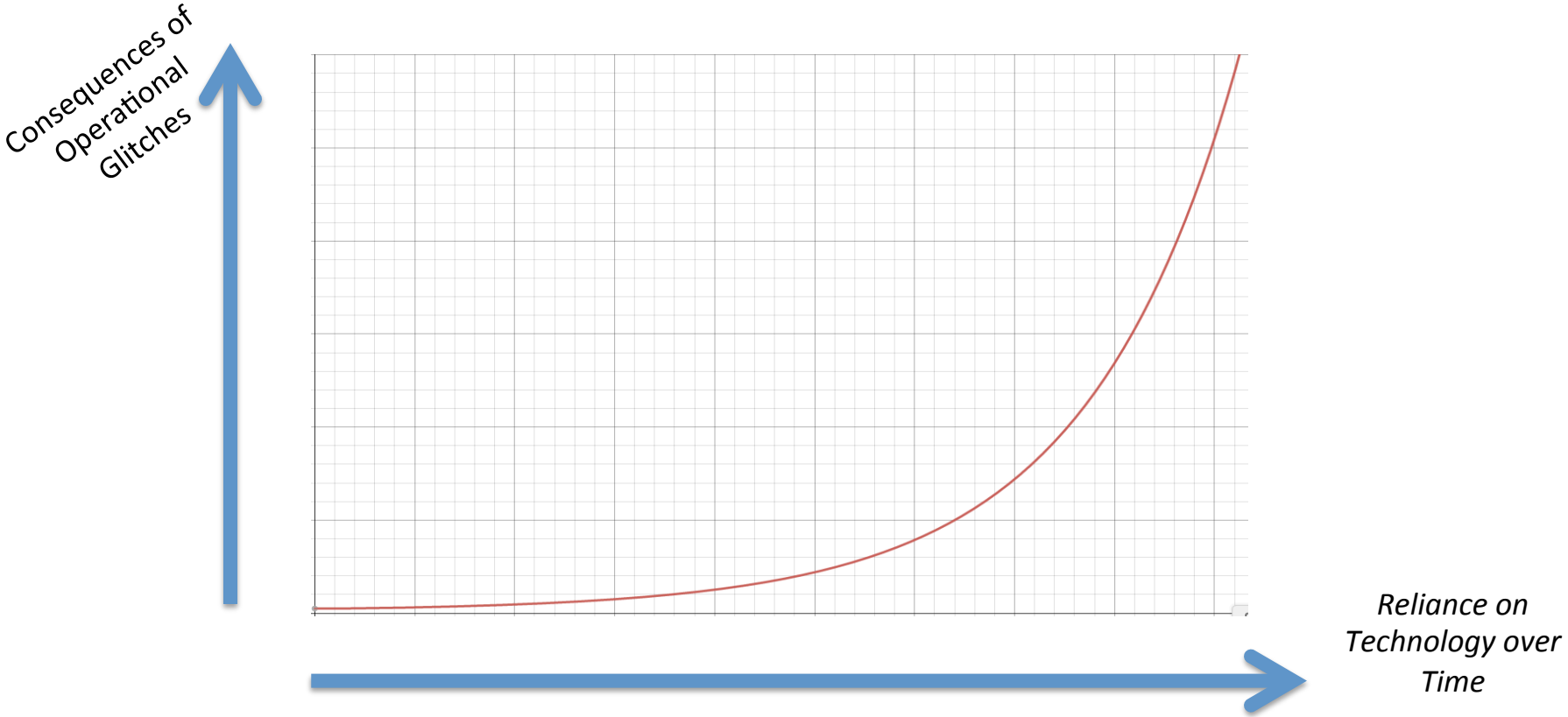
redhat.

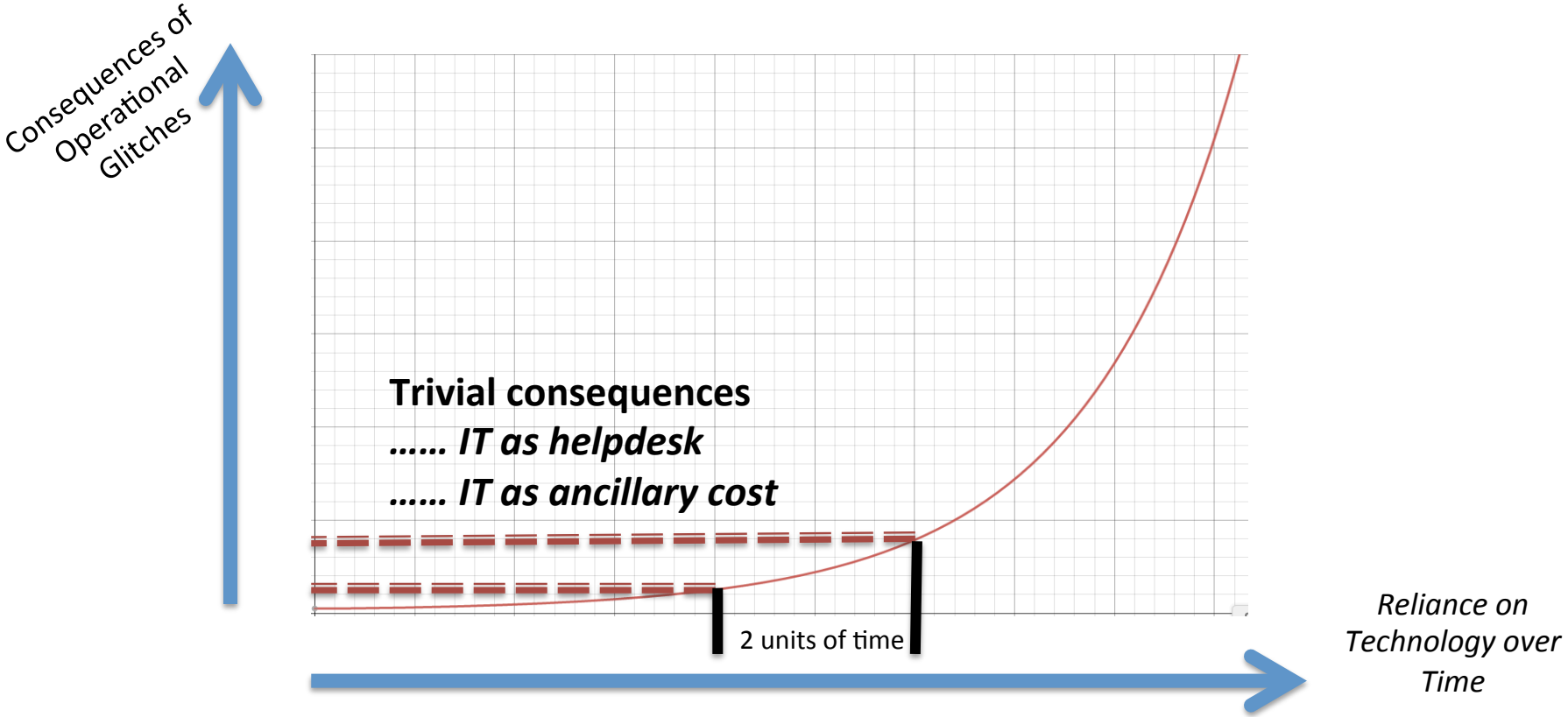
50 MINUTES, 3 GOALS (+10MIN Q&A)

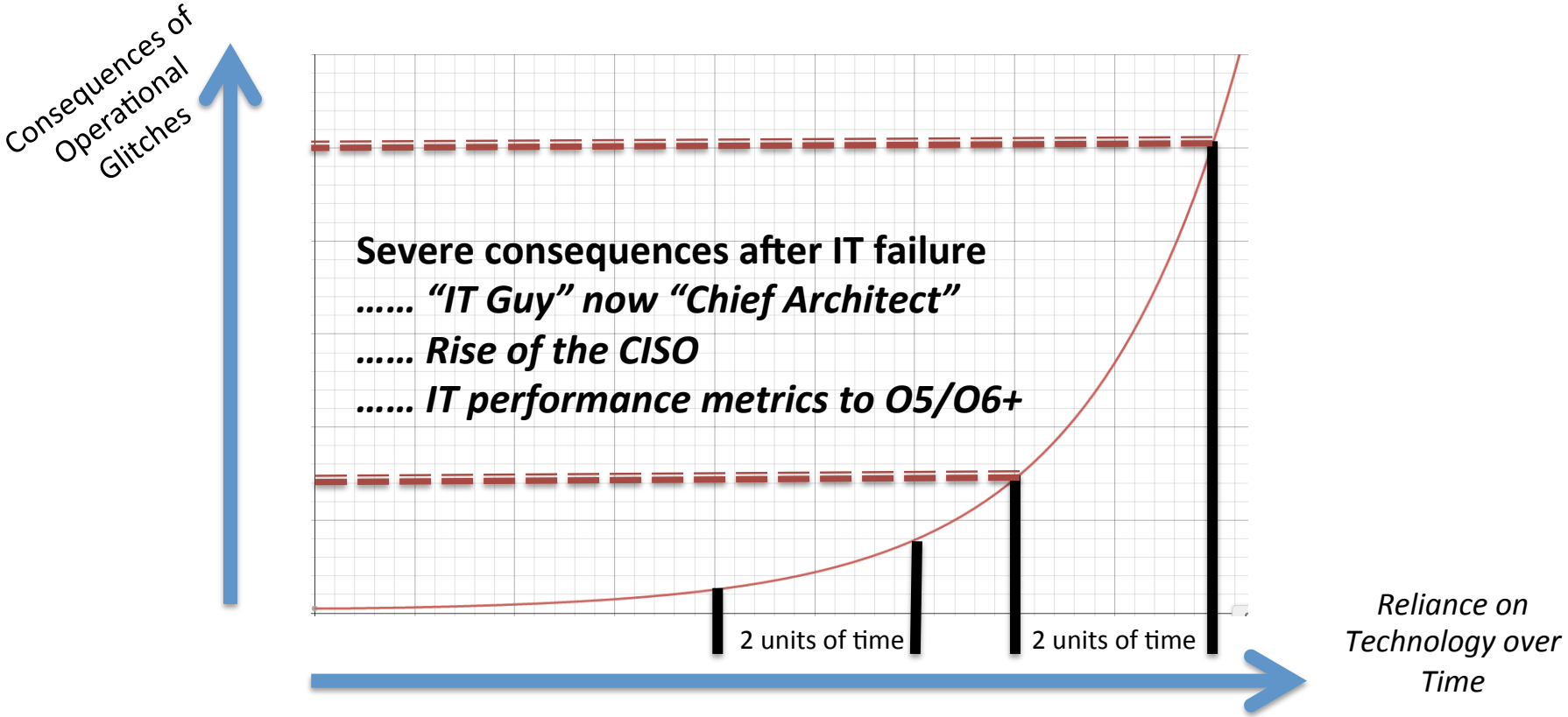
1. Discuss existing & emerging technologies for continuous monitoring
   - Vulnerability Management
   - Configuration Management

2. Share DoD Centralized Super Computing Facility story

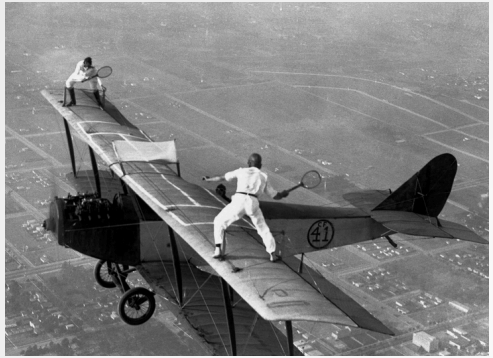
3. Data standardization technologies


Consequences of Operational Glitches
Reliance on Technology over Time


Consequences of Operational Glitches
Trivial consequences
…… IT as helpdesk
…… IT as ancillary cost
2 units of time
Reliance on Technology over Time


Consequences of Operational Glitches
Severe consequences after IT failure
…… "IT Guy" now "Chief Architect"
…… Rise of the CISO
…… IT performance metrics to O5/O6+
2 units of time
2 units of time
Reliance on Technology over Time

Ever-Increasing Capability & Complexity

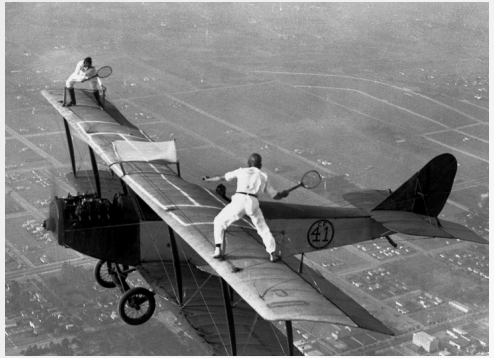


Biplane: 0 LOC

FUNCTIONALITY & COMPLEXITY

OPERATIONAL RISK

Ever-Increasing Capability & Complexity



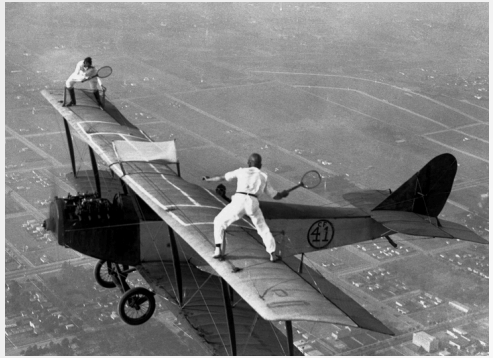
Biplane: 0 LOC

Lunar Module: 2K LOC

FUNCTIONALITY & COMPLEXITY

OPERATIONAL RISK

Ever-Increasing Capability & Complexity



Biplane: 0 LOC

Lunar Module: 2K LOC

F-35: 9.9M LOC

FUNCTIONALITY & COMPLEXITY

OPERATIONAL RISK


AP
The Associated Press
@AP
Following
Breaking: Two Explosions in the White House and Barack Obama is injured
Reply
Retweet
Favorite
More
1,849
RETWEETS
82
FAVORITES
1:07 PM - 23 Apr 13

INDU ↓ 14690.06 +122.89 14688.12/14692.81
At 13:34 O 14567.17 H 14720.34 L 14554.29 Prev 14567.17

INDU Index | 95) Save As | 96) Actions | 97) Edit | Intraday Chart

1 day(s) 04/23/2013 - 04/23/2013 09:30 - 14:15 Trade 11) Compare USD

1D 3D 1M 6M YTD 1Y 5Y Max Tick ▼ Security/Study Event

Track Annotate News Zoom

14720
14700
14690.06
14680
14660
14640
14620
14600
14580
14560

12:30 13:00 13:30 14:00

The Associated Press
@AP

Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

579 RETWEETS 19 FAVORITES

Sections ≡ The Washington Post Search MERRILL EDGE Sign In Subscribe

Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?

A 2

By Max Fisher April 23, 2013 Follow @Max_Fisher

Country Reports on Terrorism 2013

April 2014

United States Department of State Publication
Bureau of Counterterrorism
Released April 2014

Country Reports on Terrorism 2013 is submitted in compliance with Title 22 of the United States Code, Section 2656f (the "Act"), which requires the Department of State to provide to Congress a full and complete annual report on terrorism for those countries and groups meeting the criteria of the Act.

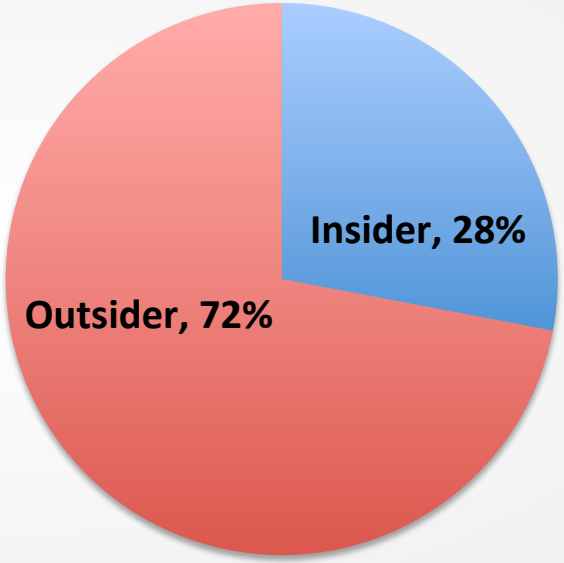
http://www.state.gov/documents/organization/225886.pdf

"In April 2013, AQI's leader Abu Bakr al-Baghdadi declared the group was operating in Syria and changed its public name to the Islamic State of Iraq and the Levant(ISIL)."

"On April 30, the U.S. State Department noted that private donations from Persian Gulf countries were "a major source of funding for Sunni terrorist groups, particularly...in Syria," calling the problem one of the most important counterterrorism issues during the previous calendar year. Groups such as al-Qaeda's Syrian affiliate, Jabhat al-Nusra, and the Islamic State of Iraq and al-Sham (ISIS), previously known as al-Qaeda in Iraq, are believed to be frequent recipients of some of the hundreds of millions of dollars that wealthy citizens and others in the Gulf peninsula have been donating during the Syrian conflict."

2014 U.S. State of Cybercrime Survey

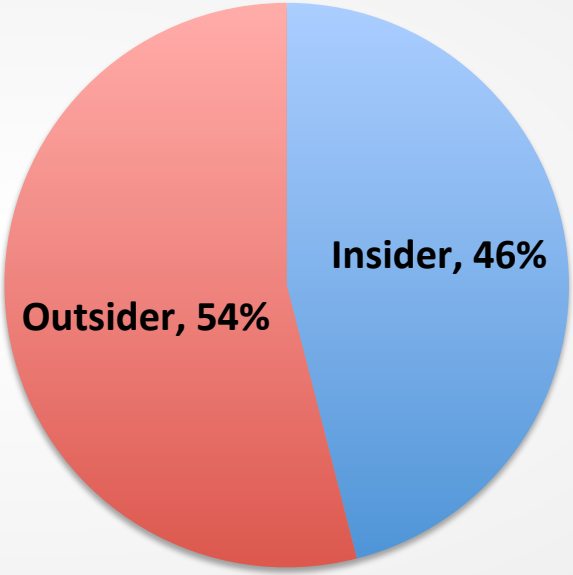
What percent of Electronic Crime events are known or suspected to have been caused by . . .



Source: 2014 US State of Cybercrime Survey, CSO Magazine
(sponsored by Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014)

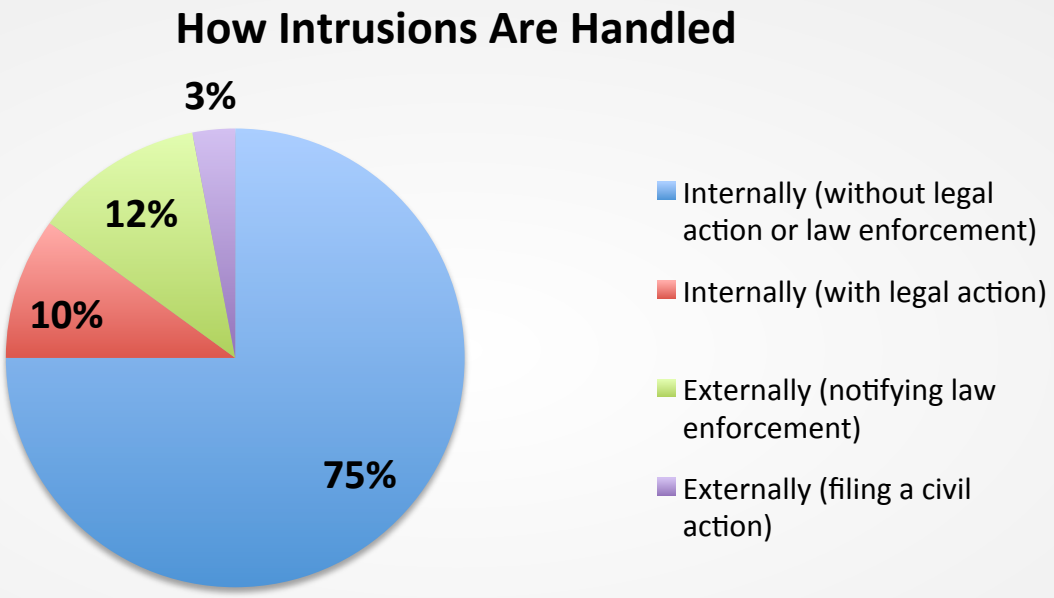
2014 U.S. State of Cybercrime Survey

Which Electronic Crimes were more costly or damaging to your organization, those perpetrated by . . .



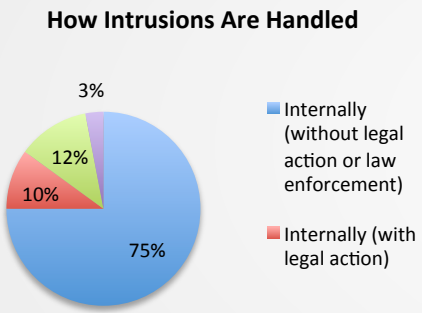
Source: 2014 US State of Cybercrime Survey, CSO Magazine
(sponsored by Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014)

2014 U.S. State of Cybercrime Survey



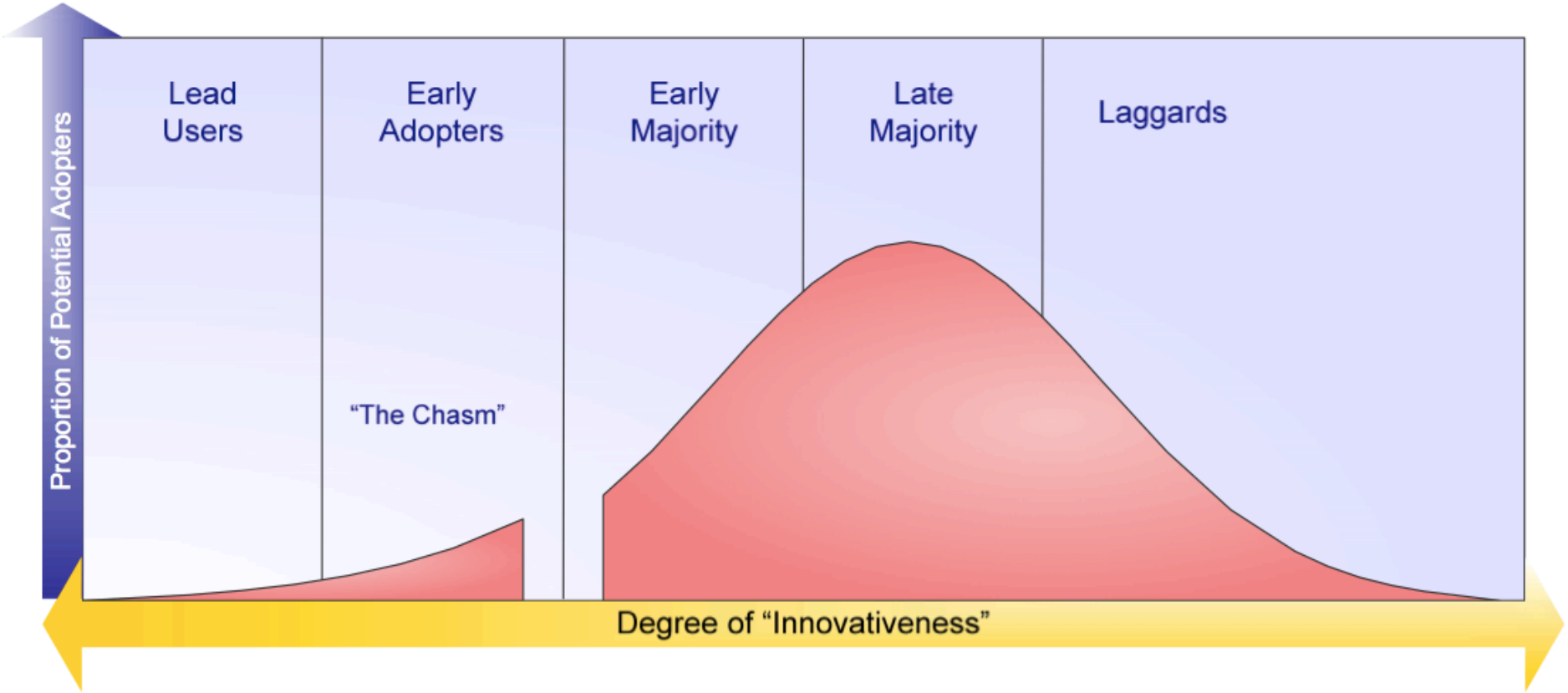
Source: 2014 US State of Cybercrime Survey, CSO Magazine
(sponsored by Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014)

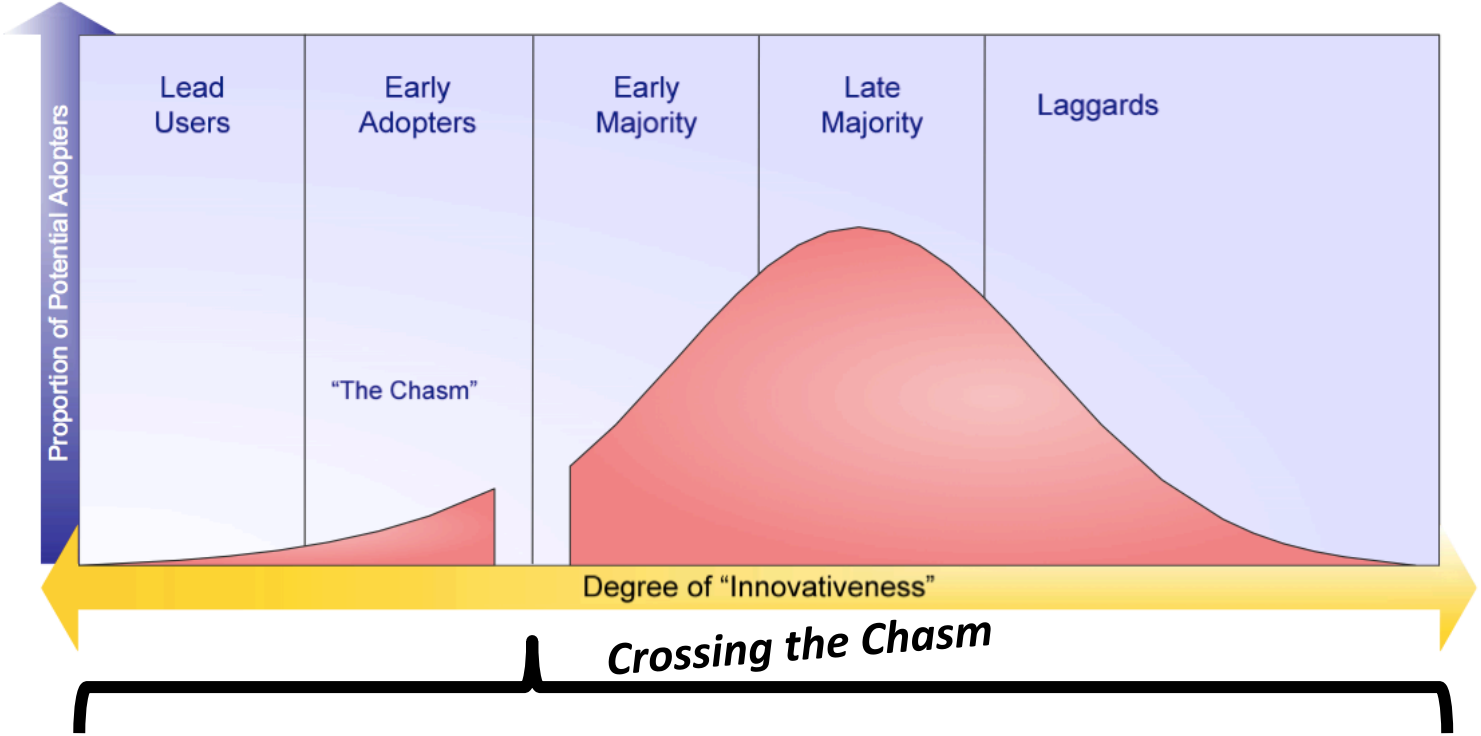
2014 U.S. State of Cybercrime Survey

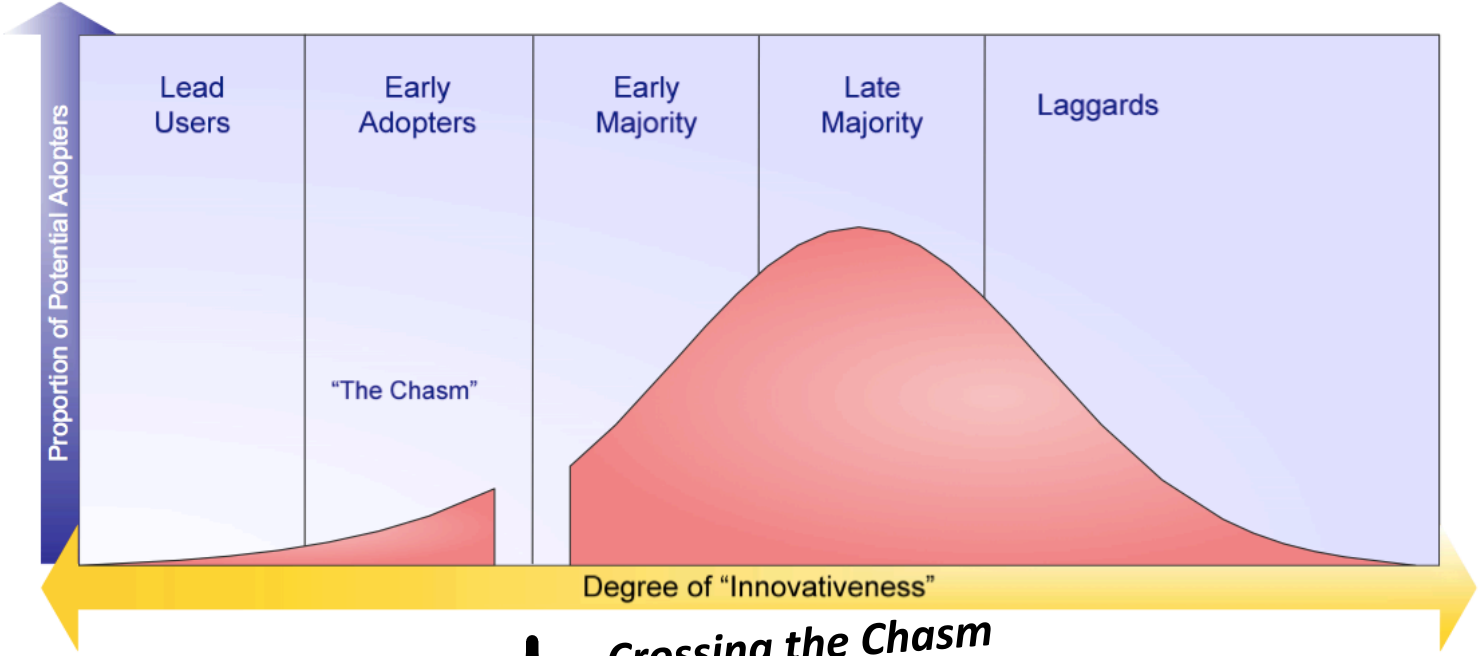


Top 5 Reasons Cyber Crimes were not referred for legal action	
Damage level insufficient to warrant prosecution	34%
Lack of evidence/not enough information to prosecute	36%
Could not identify the individuals responsible	37%
Negative publicity	12%
Don't know	21%

Source: 2014 US State of Cybercrime Survey, CSO Magazine
(sponsored by Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014)

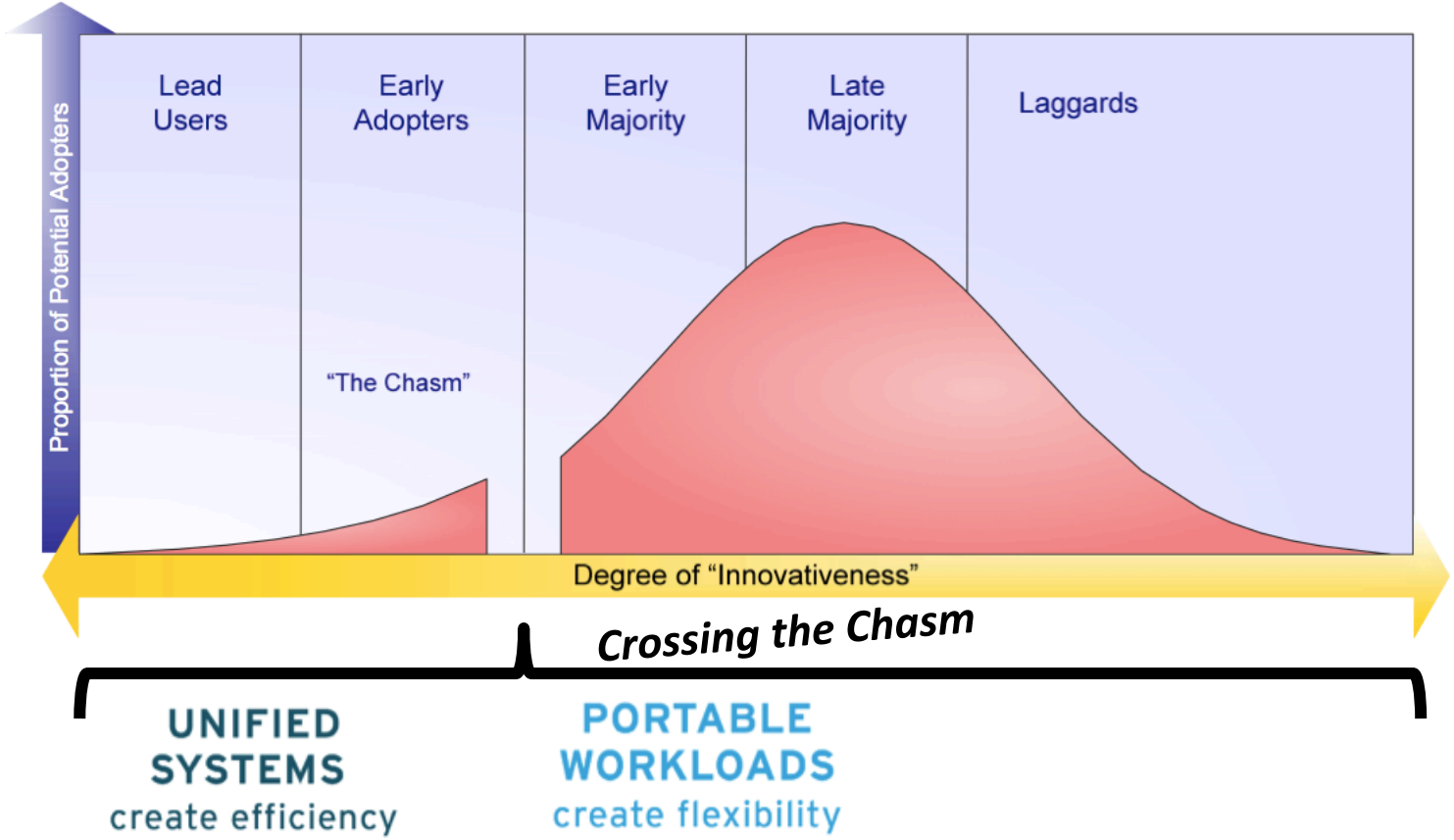

Lead Users
Early Adopters
Early Majority
Late Majority
Laggards
"The Chasm"
Proportion of Potential Adopters
Degree of "Innovativeness"

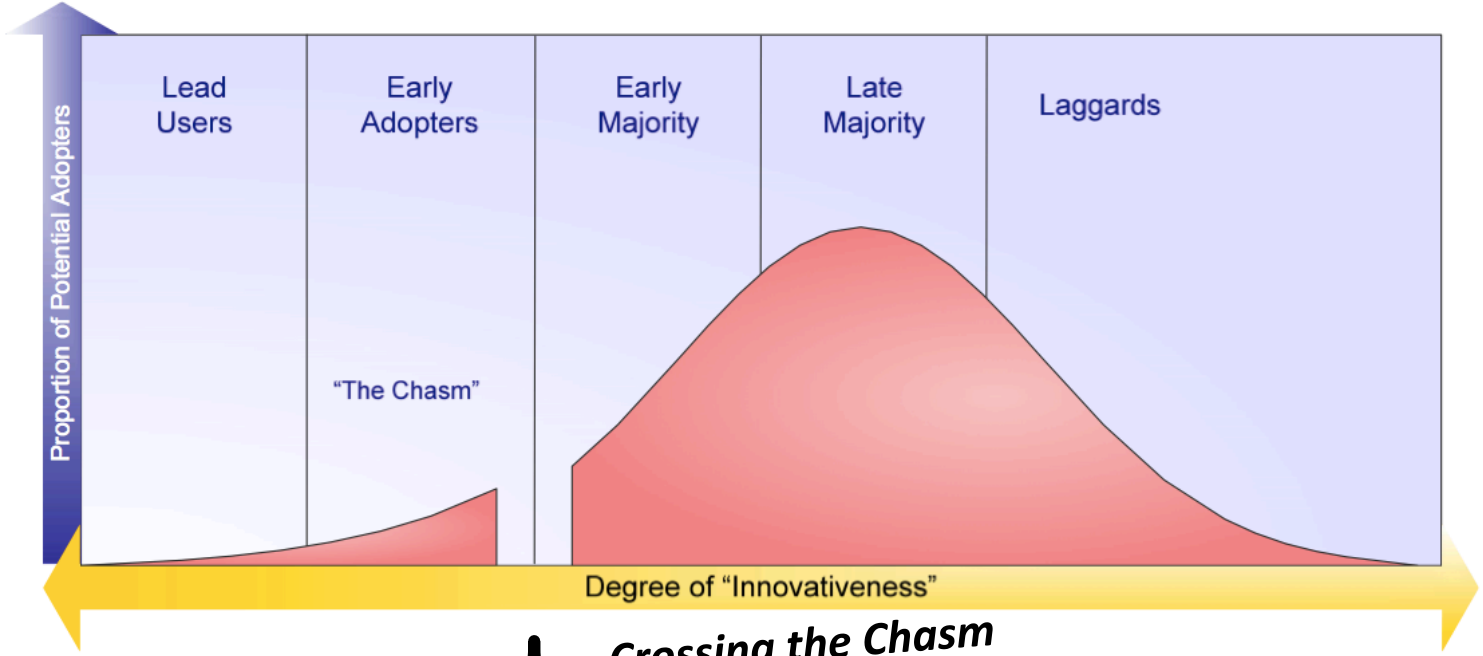

Lead Users
Early Adopters
Early Majority
Late Majority
Laggards
"The Chasm"
Proportion of Potential Adopters
Degree of "Innovativeness"
Crossing the Chasm



Crossing the Chasm

UNIFIED SYSTEMS
create efficiency


Proportion of Potential Adopters
Lead Users
Early Adopters
Early Majority
Late Majority
Laggards
"The Chasm"
Degree of "Innovativeness"
Crossing the Chasm
UNIFIED SYSTEMS
create efficiency
PORTABLE WORKLOADS
create flexibility

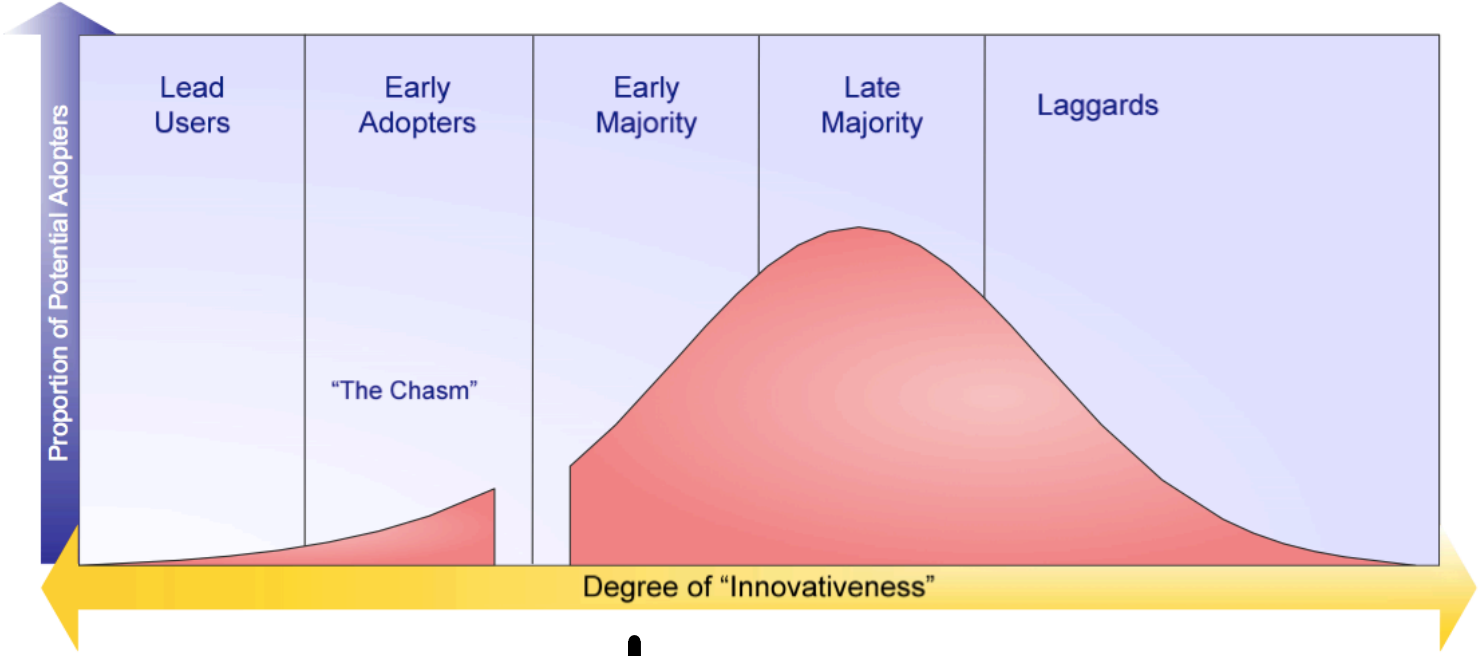


Crossing the Chasm

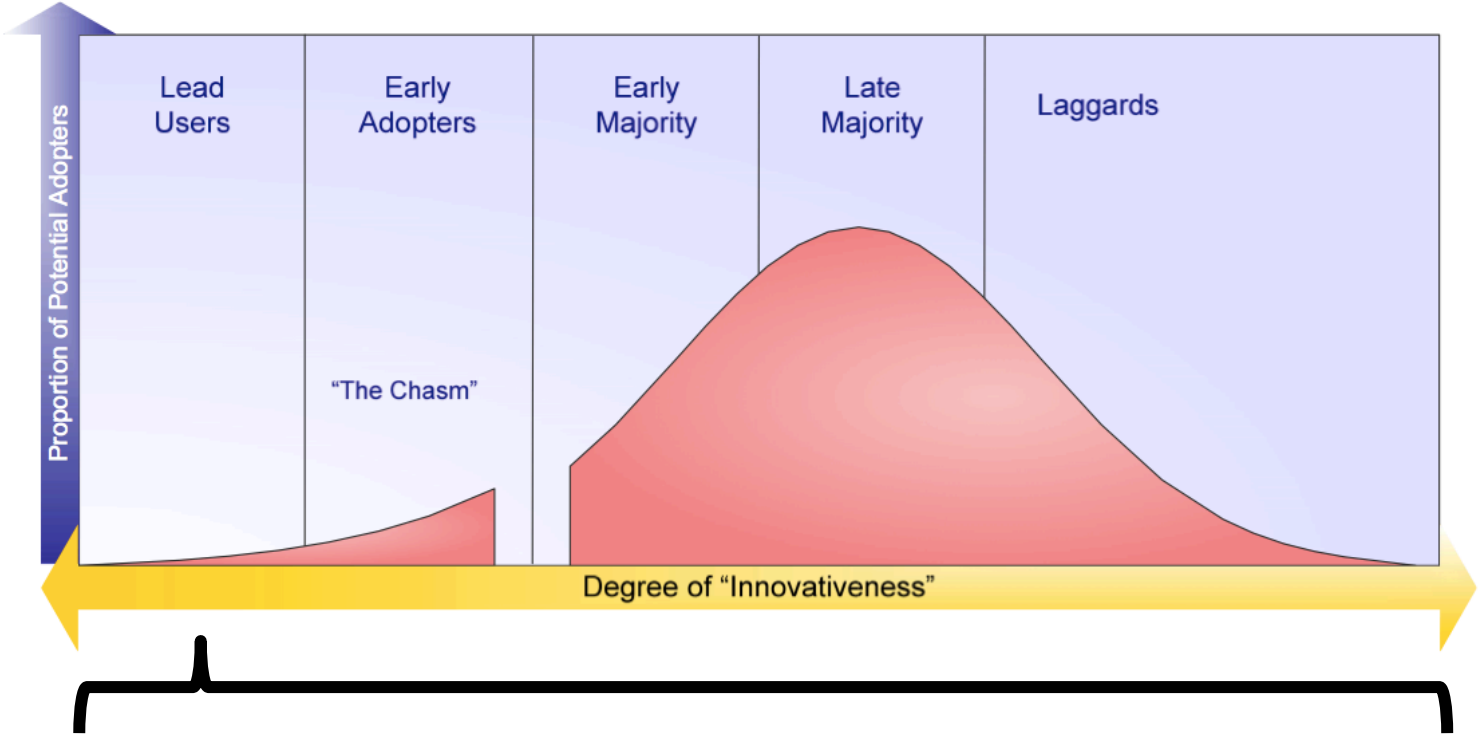
UNIFIED SYSTEMS
create efficiency

PORTABLE WORKLOADS
create flexibility

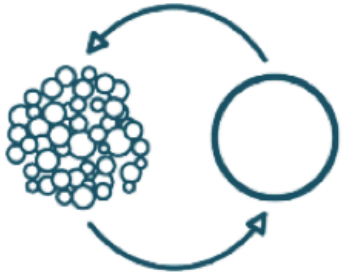
OPEN STANDARDS
ensure your organization is future-proof



Case Study:
U.S. Department of Defense
Centralized Super Computing Facility



"Innovation Programs" – Review of ongoing work with NSA's Information Assurance Directorate and NIST



UNIFIED SYSTEMS
create efficiency

PORTABLE WORKLOADS
create flexibility

OPEN STANDARDS
ensure your organization is future-proof

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

Statement of Robert F. Dacey
Director, Information Security Issues

http://www.gao.gov/assets/120/110329.pdf

"80% of attacks leverage known vulnerabilities and configuration management setting weaknesses"

UNIFIED SYSTEMS

- LOWERING RISK
  - Correcting “tunnel vision”
  -
  -
  -
-
  -
  -
  -

UNIFIED SYSTEMS

- LOWERING RISK
  - Correcting “tunnel vision”
  - Using math and statistics to accelerate corrective action
  -
  -

-
  -
  -
  -

UNIFIED SYSTEMS

- LOWERING RISK
  - Correcting “tunnel vision”
  - Using math and statistics to accelerate corrective action
  - Daily risk calculations/priorities
  -

-
  -
  -
  -

UNIFIED SYSTEMS

- LOWERING RISK
  - Correcting “tunnel vision”
  - Using math and statistics to accelerate corrective action
  - Daily risk calculations/priorities
  - Automated business processes (patch distribution, corrective actions, etc)

- … WHILE NOT CHANGING
  - Structure of departments or agencies
  - Decentralized technology management
  - Structure of security program

UNIFIED SYSTEMS

- LOWERING RISK
  - Correcting “tunnel vision”
  - Using math and statistics to accelerate corrective action
  - Daily risk calculations/priorities
  - Automated business processes (patch distribution, corrective actions, etc)

- … WHILE NOT CHANGING
  - Structure of departments or agencies
  - Decentralized technology management
  - Structure of security program

OBSTACLE:

CxO’s accountable for IT security

BUT

Directly supervise only a small % of systems in use

Framework:

1. **Scan every 36-72 hours**
2. Focus on Attack Readiness
3. **Find & Fix Top Issues Daily**
4. Personal results graded
5. **Hold managers responsible**

An SCAP Primer

- Security Content Automation Protocol (SCAP)

An SCAP Primer

- Security Content Automation Protocol (SCAP)

- Defines standardized formats
  - Standardized inputs (e.g. a compliance baseline, status query)
  - Standardized outputs (machine readable results)

  - *NIST 800-117: Guide to Adopting and Using the Security Content Automation Protocol*
  - *NIST 800-126: The Technical Specification for the Security Content Automation Protocol*

  - *NIST IR 7511: Requirements for vendors to attain NIST Validation*

An SCAP Primer

- Security Content Automation Protocol (SCAP)

- Defines standardized formats
  - Standardized inputs (e.g. a compliance baseline, status query)
  - Standardized outputs (machine readable results)

- Provides the DoD enterprise with *liberty* with regard to product choices
  - Avoids vendor lock-in, enables interoperability
  - Provides common technical position to vendors, integrators, mission partners
  - Federal procurement language requires SCAP support in some cases (e.g. new Common Criteria language)

SCAP Security Guide

https://github.com/OpenSCAP/scap-security-guide

Contributors include . . .

Live Demo

SCAP Security Guide

- ~1.66M lines of code from 80 developers across DoD, IC, Civilian, industry, academia
- NIST Validated tooling (OpenSCAP)
- Upstream for US Gov Enterprise Linux baselines
  - STIG: DoD RHEL6 baseline, produced by DISA FSO
  - C2S: Intelligence Community “Commercial Cloud” for JWICS
  - CSCF: NRO’s Centralized Super Computing Facility (CNSSI 1253 controls)
  - CS2: NSA RHEL6 baseline
  - US Navy JBoss EAP
- Shipping *natively* in Enterprise Linux

2.4.2.4.b. Set Password Hashing Algorithm in /etc/login.defs

In `/etc/login.defs`, add or correct the following line to ensure the system will use SHA-512 as the hashing algorithm:

```
ENCRYPT_METHOD SHA512
```

Using a stronger hashing algorithm makes password cracking attacks more difficult.

Remediation script

```
                        if grep --silent ^ENCRYPT_METHOD /etc/login.defs ; then
        sed -i 's/^ENCRYPT_METHOD.*/ENCRYPT_METHOD SHA512/g' /etc/login.defs
else
        echo "" >> /etc/login.defs
        echo "ENCRYPT_METHOD SHA512" >> /etc/login.defs
fi
```

Security identifiers

- CCE-27228-6

References

1. *IA-5(b)*. URL: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
2. *IA-5(c)*. URL: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
3. *IA-5(1)(c)*. URL: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
4. *IA-7*. URL: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
5. *803*. URL: <http://iase.disa.mil/cci/index.html>.

SRG-OS-000030	CCI-000058	The operating system must provide the capability for users to directly initiate session lock mechanisms.	A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the system but does not want to log out because of the temporary nature of the absence. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users may secure their account should the need arise for them to temporarily vacate the immediate physical vicinity.	Install the screen Package	To enable console screen locking, install the `screen` package:
					`$ sudo yum install screen`
					Instruct users to begin new terminal sessions with the following command:
					`$ screen`
					The console can now be locked with the following key combination:
					`ctrl+a x`

SRG-OS-000031	CCI-000060	The operating system session lock mechanism, when activated on a device with a display screen, must place a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.	A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the system but does not log out because of the temporary nature of the absence. The session lock will also include an obfuscation of the display screen to prevent other users from reading what was previously displayed.	Implement Blank Screensaver	Run the following command to set the screensaver mode in the GNOME desktop to a blank screen:
					`$ sudo gconftool-2 --direct \`
					`  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \`
					`  --type string \`
					`  --set /apps/gnome-screensaver/mode blank-only`

SRG-OS-000032	CCI-000067	The operating system must employ automated mechanisms to facilitate the monitoring and control of remote access methods.	Remote network access is accomplished by leveraging common communication protocols and establishing a remote connection. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.	Enable auditd Service	The `auditd` service is an essential userspace component of the Linux Auditing System, as it is responsible for writing audit records to disk. The `auditd` service can be enabled with the following command: `# chkconfig --level 2345 auditd on`

AC-19(e)	Disable GNOME Automounting	The system's default desktop environment, GNOME, will mount devices and remo inserted into the system. Disable automount and autorun within GNOME by runn
		
		`# gconftool-2 --direct \`
		`  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory`
		`  --type bool \`
		`  --set /apps/nautilus/preferences/media_automount false`
		`# gconftool-2 --direct \`
		`  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory`
		`  --type bool \`
		`  --set /apps/nautilus/preferences/media_autorun_never true`
		
		These settings can be verified by running the following:
		
		`$ gconftool-2 --direct \`
		`  --config-source xml:read:/etc/gconf/gconf.xml.mandatory \`
		`  --get /apps/nautilus/preferences/media_automount`
		`$ gconftool-2 --direct \`
		`  --config-source xml:read:/etc/gconf/gconf.xml.mandatory \`
		`  --get /apps/nautilus/preferences/media_autorun_never`

CM-7	Disable Mounting of cramfs	To configure the system to prevent the `cramfs` kernel module from being loaded, `install cramfs /bin/false` This effectively prevents usage of this uncommon filesystem.
CM-7	Disable Mounting of freevxfs	To configure the system to prevent the `freevxfs` kernel module from being loade `install freevxfs /bin/false` This effectively prevents usage of this uncommon filesystem.
CM-7	Disable Mounting of jffs2	To configure the system to prevent the `jffs2` kernel module from being loaded, a `install jffs2 /bin/false` This effectively prevents usage of this uncommon filesystem.

XCCDF results

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	tota
7	0	4	2	0	4	0	0	0	1

Title	Result
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	pass
Direct root Logins Not Allowed	notchecked
Restrict Virtual Console Root Logins	error
Restrict Serial Port Root Logins	error
Restrict Web Browser Use for Administrative Accounts	notchecked
Ensure that System Accounts Do Not Run a Shell Upon Login	pass
Verify Only Root Has UID 0	pass
Root Path Must Be Vendor Default	notchecked
Prevent Log In to Accounts With Empty Password	fail
Verify All Account Password Hashes are Shadowed	pass
All GIDs referenced in /etc/passwd must be defined in /etc/group	notchecked
Verify No netrc Files Exist	pass
Set Password Minimum Length in login.defs	fail
Set Password Minimum Age	fail
Set Password Maximum Age	fail

Save XCCDF Result | Save ARF | Open HTML report | Save HTML report | Close

Result for Install AIDE

Result: **pass**

Rule ID: **package_aide_installed**

Time: **2014-12-14 01:15**

Severity: **medium**

Install the AIDE package with the command:

```
# yum install aide
```

The AIDE package must be installed if it is to be available for integrity checking.

Security identifiers

- CCE-27024-9

Remediation script

```
yum -y install aide
```

```
<rule-result idref="package_aide_installed" time="2014-04-16T05:39:00" severity="medium" weight="1.000000">
  <result>fail</result>
  <ident system="http://cce.mitre.org">CCE-27024-9</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
  </check>
</rule-result>
```

```
<rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
    The AIDE package must be installed if it is to be available for integrity checking.
</rationale>
<ident system="http://cce.mitre.org">CCE-27024-9</ident>
<fix xmlns:xhtml="http://www.w3.org/1999/xhtml" system="urn:xccdf:fix:script:sh">
    yum -y install aide
</fix>
<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
</check>
```

```
<rule-result idref="package_aide_installed" time="2014-04-16T05:39:00" severity="medium" weight="1.000000">
  <result>fail</result>
  <ident system="http://cce.mitre.org">CCE-27024-9</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
  </check>
</rule-result>
<rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
    The AIDE package must be installed if it is to be available for integrity checking.
</rationale>
<ident system="http://cce.mitre.org">CCE-27024-9</ident>
<fix xmlns:xhtml="http://www.w3.org/1999/xhtml" system="urn:xccdf:fix:script:sh">
    yum -y install aide
</fix>
<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
</check>
```

```
<rule-result idref="package_aide_installed" time="2014-04-16T05:39:00" severity="medium" weight="1.000000">
  <result>fail</result>
  <ident system="http://cce.mitre.org">CCE-27024-9</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
  </check>
</rule-result>
 <rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
     The AIDE package must be installed if it is to be available for integrity checking.
 </rationale>
 <ident system="http://cce.mitre.org">CCE-27024-9</ident>
 <fix xmlns:xhtml="http://www.w3.org/1999/xhtml" system="urn:xccdf:fix:script:sh">
     yum -y install aide
 </fix>
 <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
   <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
 </check>
```

```
<rule-result idref="package_aide_installed" time="2014-04-16T05:39:00" severity="medium" weight="1.000000">
  <result>fail</result>
  <ident system="http://cce.mitre.org">CCE-27024-9</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
  </check>
</rule-result>
```

```
<rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
    The AIDE package must be installed in order to be available for integrity checking.
</rationale>
<ident system="http://cce.mitre.org">CCE-27024-9</ident>
<fix xmlns:xhtml="http://www.w3.org/1999/xhtml" system="urn:xccdf:fix:script:sh">
    yum -y install aide
</fix>
<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref name="oval:ssg:def:244" href="ssg-rhel6-oval.xml"/>
</check>
```

oval:com.redhat.rhsa:def:20130744	true	patch	RHSA-2013:0744-01 CVE-2012-6537 CVE-2012-6538 CVE-2012-6546 CVE-2012-6547 CVE-2013-0349 CVE-2013-0913 CVE-2013-1767 CVE-2013-1773 CVE-2013-1774 CVE-2013-1792 CVE-2013-1796 CVE-2013-1797 CVE-2013-1798 CVE-2013-1826 CVE-2013-1827	RHSA-2013:0744: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20130898	false	patch	RHSA-2013:0898-00 CVE-2013-1993	RHSA-2013:0898: mesa security update (Moderate)
oval:com.redhat.rhsa:def:20130896	false	patch	RHSA-2013:0896-00 CVE-2013-2007	RHSA-2013:0896: qemu-kvm security and bug fix update (Moderate)

SCAP Deployment: CSCF

- Established September 1985 to provide HPC resources for use by the classified NRT and scientific computing communities
  - DS&T was facilitator with SMUG committee of user groups
  - WF took over with consolidation of WF to current management

- CSCF is currently located in ADF-E
  - Applications support – code optimization, code parallelization, conversion, algorithm development/modification
  - O&M support – OS configuration, help desk, backups, disaster recovery, etc

SCAP Deployment: CSCF

- CSCF followed the ICD 503 Six steps with standard controls and Cross Domain System (CDS) controls (CDS is approximately equal to MLS)
- Controls were straight forward
- Testing was very problematic
  - Testers unfamiliar with Linux, much less MLS.
  - Test Output Formatting
    - CSCF moving to SCAP with Red Hat using the xml and html outputs to standardize on with Red Hat support

INSTALLATION SUMMARY

FEDORA 19 INSTALLATION
PRE-RELEASE / TESTING

us

LOCALIZATION

DATE & TIME
Europe/Prague timezone

KEYBOARD
English (English (US))

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY PROFILE
Misconfiguration detected

SOFTWARE

INSTALLATION SOURCE
Closest mirror

NETWORK CONFIGURATION
Wired (eth0) connected

SOFTWARE SELECTION
Custom software selected

STORAGE

INSTALLATION SUMMARY

FEDORA 19 INSTALLATION
PRE-RELEASE / TESTING

us

LOCALIZATION

DATE & TIME
Europe/Prague timezone

KEYBOARD
English (English (US))

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY PROFILE
Misconfiguration detected

SOFTWARE

INSTALLATION SOURCE
Closest mirror

NETWORK CONFIGURATION
Wired (eth0) connected

SOFTWARE SELECTION
Custom software selected

STORAGE

SPOKE NAME

FEDORA 19 INSTALLATION

PRE-RELEASE / TESTING

Done

us

Data stream: scap_org.open-scap_datastream_tst

Checklist: scap_org.open-scap_cref_first-xccdf.xml

Choose profile below:

My testing profile

A profile for testing purposes.

My testing profile2

Another profile for testing purposes.

Select profile

Changes that were done or need to be done:

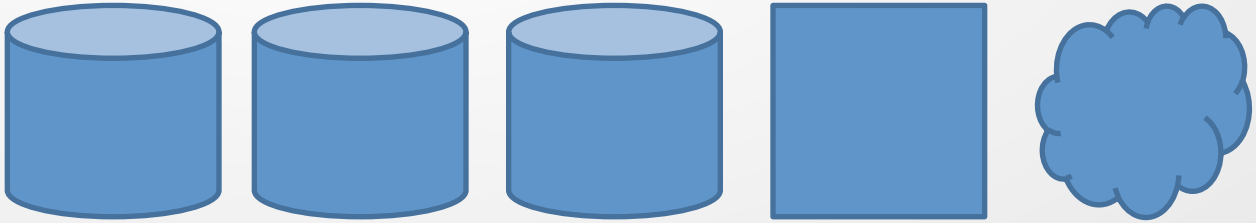
- /tmp must be on a separate partition or logical volume
- root password was too short, a longer one with at least 10 characters will be required
- package 'iptables' has been added to the list of to be installed packages
- package 'telnet' has been added to the list of excluded packages

```
1 this is a simple kickstart file for testing OSCAP addon's features
2
3 # values saving a lot of clicks in the GUI
4 lang en US.UTF-8
5 keyboard --xlayour=us --vckeymap=us
6 timezone Europe/Prague
7 rootpw aaaaa
8 bootloader --location=mbr
9 clearpart --initlabel --all
10 autopart --type=plain
11
12 %packages
13 vim
14 %end
15
16 %addon org_fedora_oscap
17         content-type = archive
18         content-url = http://192.168.122.1/xccdf_content.zip
19         profile = xccdf_com.stig-rhel6-server
20         xccdf-path = xccdf.xml
21 %end
```

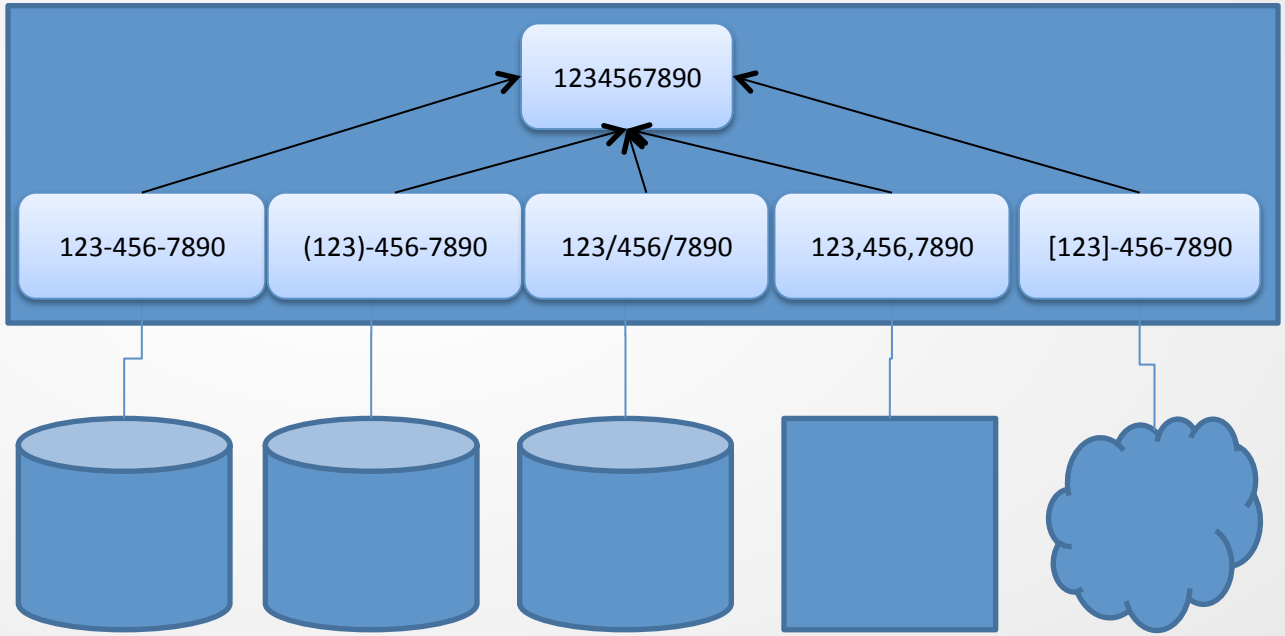
```
1  this is a simple kickstart file for testing OSCAP addon's features
2
3  # values saving a lot of clicks in the GUI
4  lang en US.UTF-8
5  keyboard --xlayour=us --vckeymap=us
6  timezone Europe/Prague
7  rootpw aaaaa
8  bootloader --location=mbr
9  clearpart --initlabel --all
10 autopart --type=plain
11
12 %packages
13 vim
14 %end
15
16 %addon org_fedora_oscap
17         content-type = archive
18         content-url = http://192.168.122.1/xccdf_content.zip
19         profile = xccdf_com.stig-rhel6-server
20         xccdf-path = xccdf.xml
21 %end
```

PORTABLE WORKLOADS

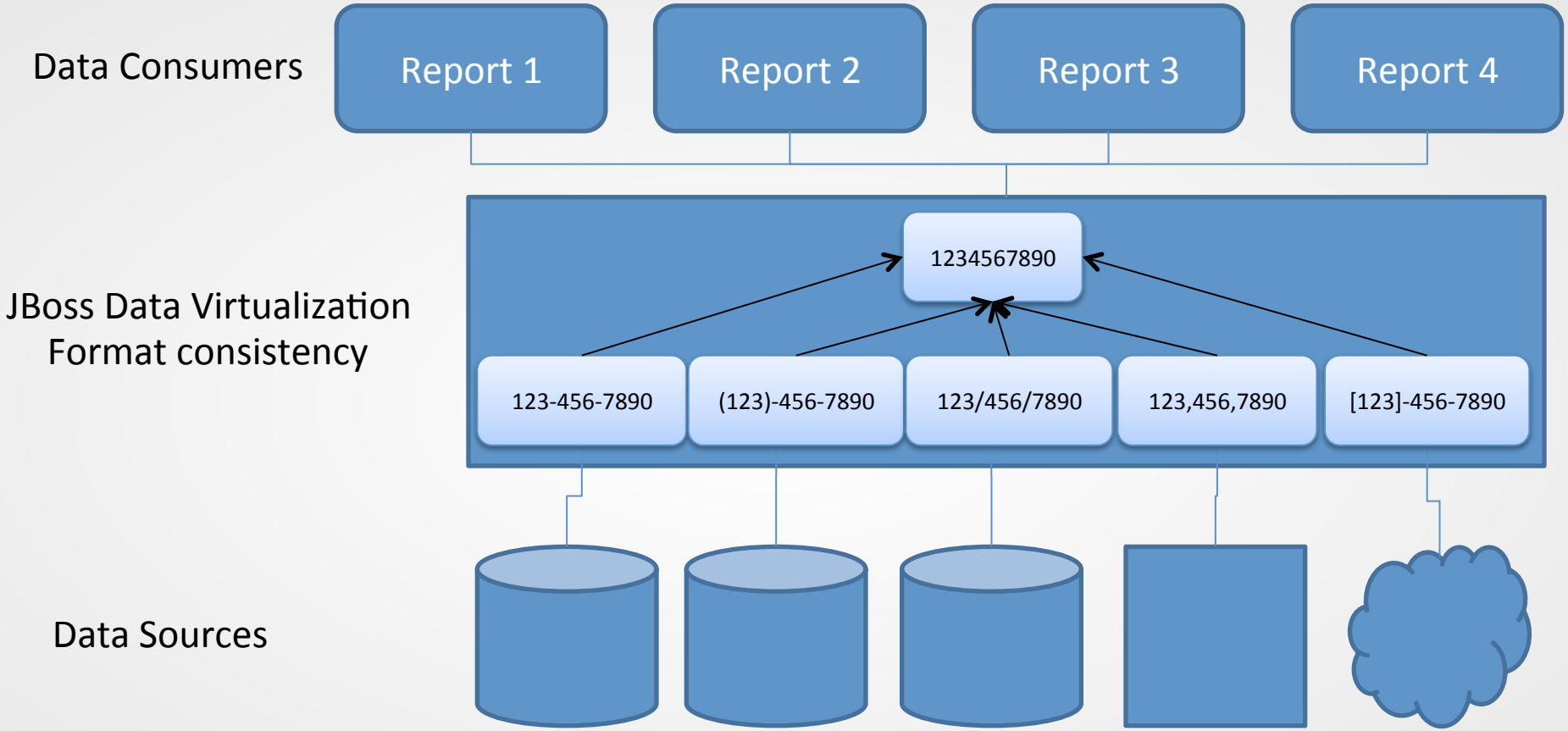
Data Sources

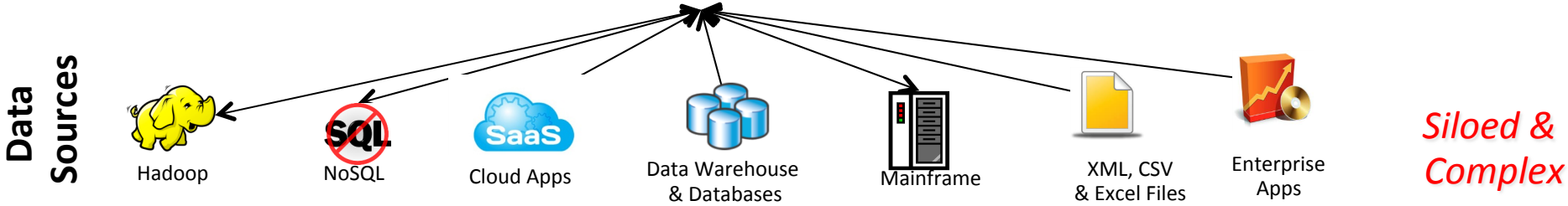


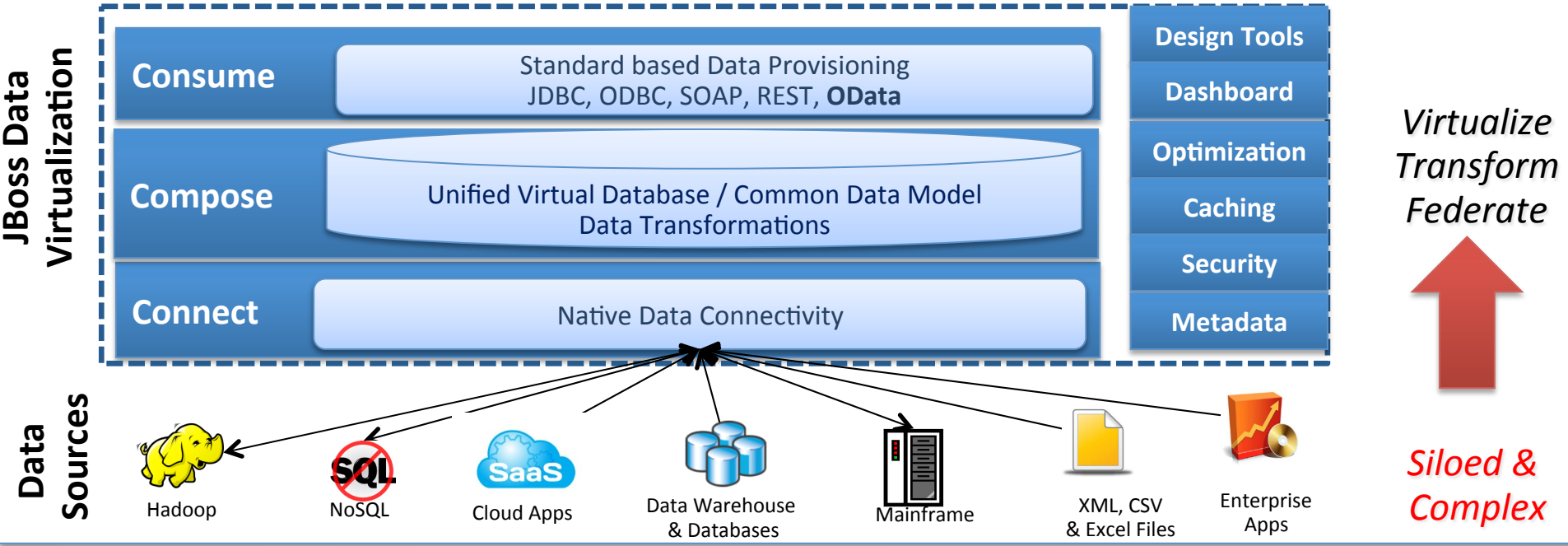
JBoss Data Virtualization
Format consistency

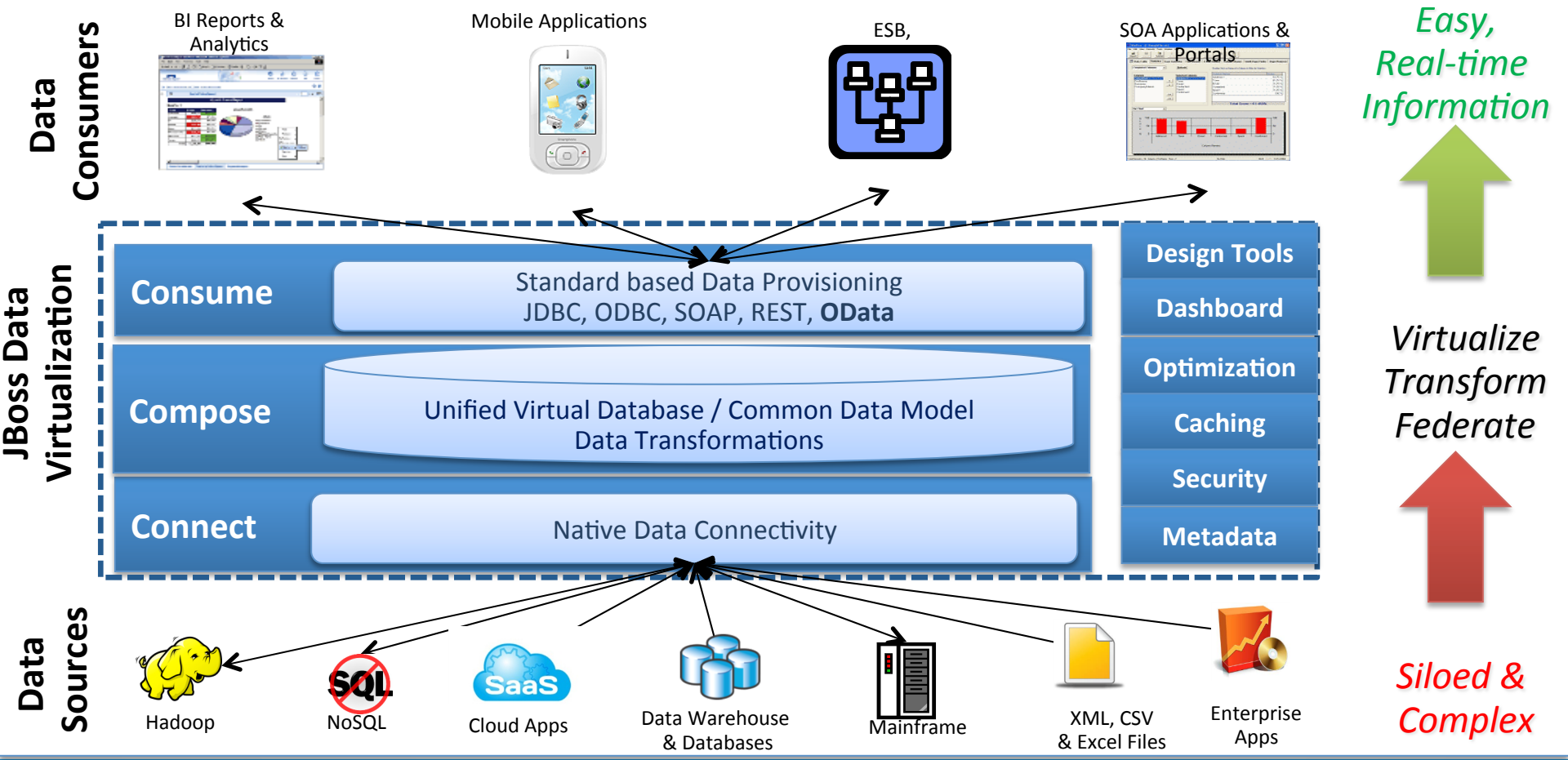


Data Sources


Data Consumers
Report 1
Report 2
Report 3
Report 4
JBoss Data Virtualization
Format consistency
1234567890
123-456-7890
(123)-456-7890
123/456/7890
123,456,7890
[123]-456-7890
Data Sources


Data Sources
Hadoop
NoSQL
Cloud Apps
Data Warehouse & Databases
Mainframe
XML, CSV & Excel Files
Enterprise Apps
Siloed & Complex


JBoss Data Virtualization
Consume
Standard based Data Provisioning
JDBC, ODBC, SOAP, REST, OData
Compose
Unified Virtual Database / Common Data Model
Data Transformations
Connect
Native Data Connectivity
Design Tools
Dashboard
Optimization
Caching
Security
Metadata
Virtualize
Transform
Federate
Data Sources
Hadoop
NoSQL
Cloud Apps
Data Warehouse & Databases
Mainframe
XML, CSV & Excel Files
Enterprise Apps
Siloed & Complex


Data Consumers
BI Reports & Analytics
Mobile Applications
ESB,
SOA Applications & Portals
Easy, Real-time Information
JBoss Data Virtualization
Consume
Standard based Data Provisioning
JDBC, ODBC, SOAP, REST, OData
Compose
Unified Virtual Database / Common Data Model
Data Transformations
Connect
Native Data Connectivity
Design Tools
Dashboard
Optimization
Caching
Security
Metadata
Virtualize
Transform
Federate
Data Sources
Hadoop
NoSQL
Cloud Apps
Data Warehouse & Databases
Mainframe
XML, CSV & Excel Files
Enterprise Apps
Siloed & Complex

JBoss by Red Hat

Logged as root Logout

Home

Sample dashboards

Sales opportunities

Expense reports

Test

Administration

Office:
- Select Office -

Department:
- Select Department -

Author:
- Select Author -

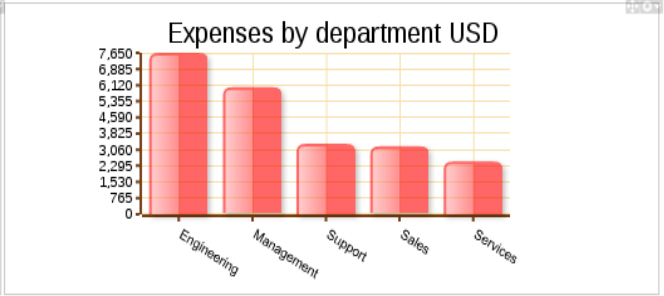
Creation date:
- Select Creation date -

Amount:
to

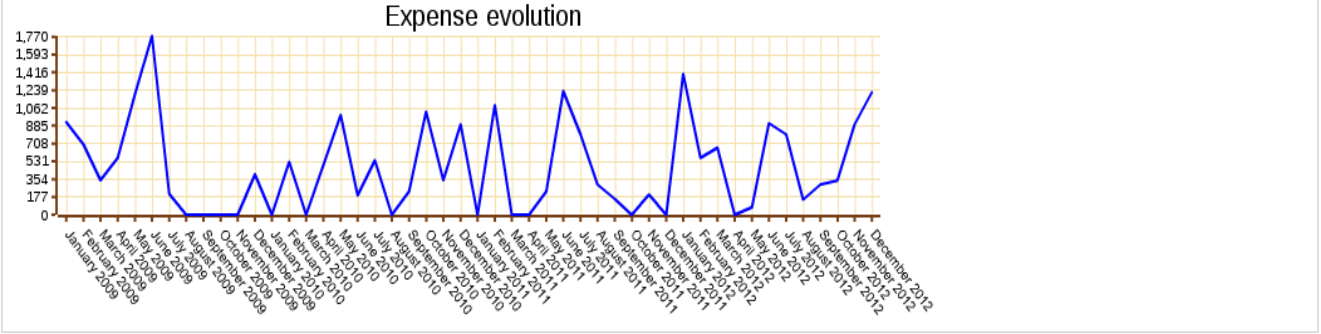
Expense Reports

Sample dashboards > Expense reports

50 Expense reports
Total amount $ 22,731.262



Expense evolution | Expenses by user | Expense reports table



Component	Risk Score	Avg	% of Score	How Component is Typically Calculated (may be overridden)
VUL - Vulnerability	982.6	3.6	16.4 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	752.0	2.7	12.6 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compli	0.0	0.0	0.0 %	From .43 for each failed Group Membership check to .9 for each failed Application Log check
AVR - Anti-Virus	240.0	0.9	4.0 %	6 per day for each signature file older than 6 days
UOS - Unapproved OS	0.0	0.0	0.0 %	100 upon detection, then 100 per month up to a maximum of 500
CSA - CyberSecurity Awareness Training	495.0	2.0	9.3 %	After 15 days past the annual training expiration date, 1 per day up to a maximum of 90
SOE - SOE Compliance	140.0	0.5	2.4 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	67.0	0.2	1.1 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	1,416.0	5.3	24.3 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS - SMS Reporting	1,250.0	4.5	20.9 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	411.0	1.5	6.9 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compli Reporting	126.0	0.5	2.1 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**5,879.6**	**21.7**	**100.0 %**	

WE CAN DO MORE WHEN WE WORK TOGETHER

Shawn Wells
Director, Innovation Programs
Red Hat Public Sector
shawn@redhat.com || 443-534-0130

redhat

DefenseNews