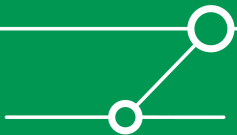
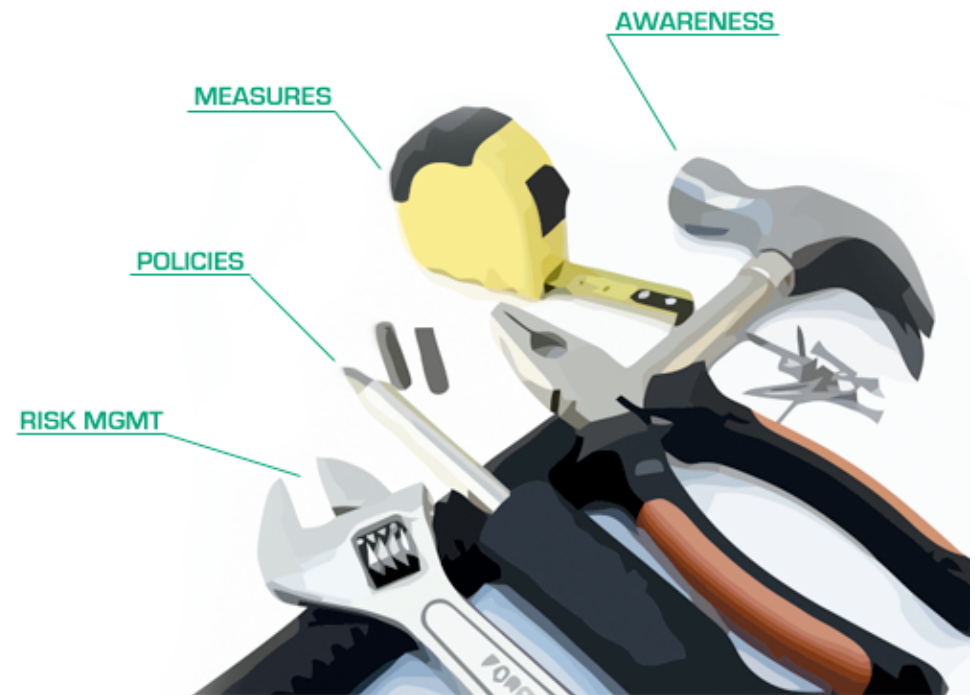


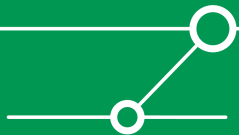
Tools of the Trade for a Modern (C)ISO

Enno Rey
erey@ernw.de

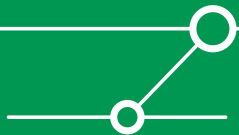


Who Am I

- **Old-school infosec guy since 1997**
- **Technical background in networking [e.g. see my ShmooCon/Day-Con talks]**
- **Security thinking centered around *risk***
- **Insinuate to a number of (C)ISOs on a regular basis [-> www.insinator.net]**
- **On a mission for a better infosec world**

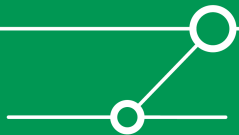


insinuator.net

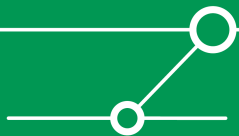


Agenda

- **This is a loose collection of thoughts on the current state of the infosec world and an ISO's role in it, covering...**
- **Tasks & Challenges of an ISO**
- **His mission & its dimensions**
- **Some movies from my youth**



Intended Audience of this Talk



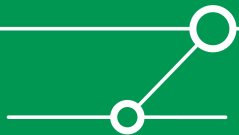
An ISO's Tasks

- **Traditional core responsibilities**

- Long-term security strategy
- Creation of policies & guidelines
- Risk assessment
- Analysis of security incidents
- Taking care of compliance...

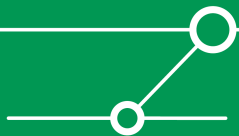


- **Main future role: *Trusted Business Advisor***

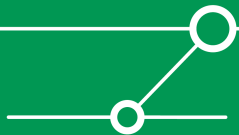
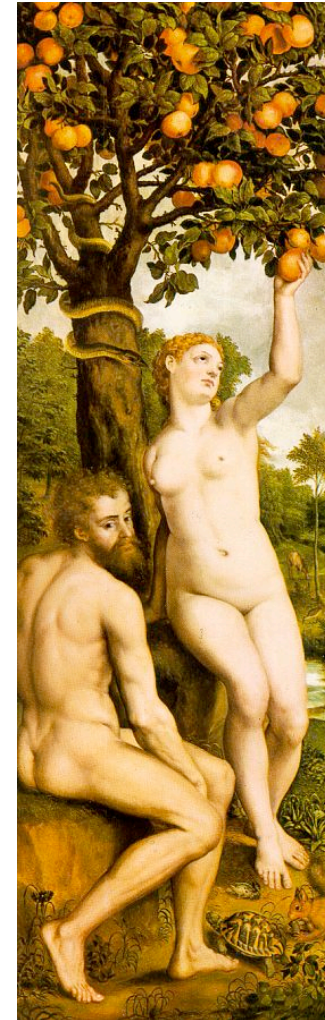


Challenges

- **World getting ever more complex**
- **Outsourcing**
- **\$NEW_Tech**
(Virtualization et.al.)
- **Limited resources**



- **All this while being despised within the organization, by a long tradition...**



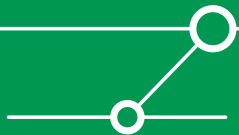
On his Ever-lasting Mission, an ISO...



Performs a constant quest for the holy grail of aligning business & infosec

Musta fight to stah the thow ever business works

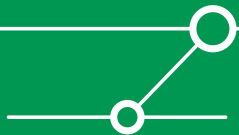
And Might even get Postal over his Impossible Task



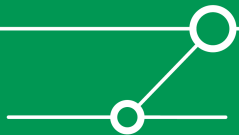
Ok, seriously, there are three Main Dimensions of an ISO's Life & Work



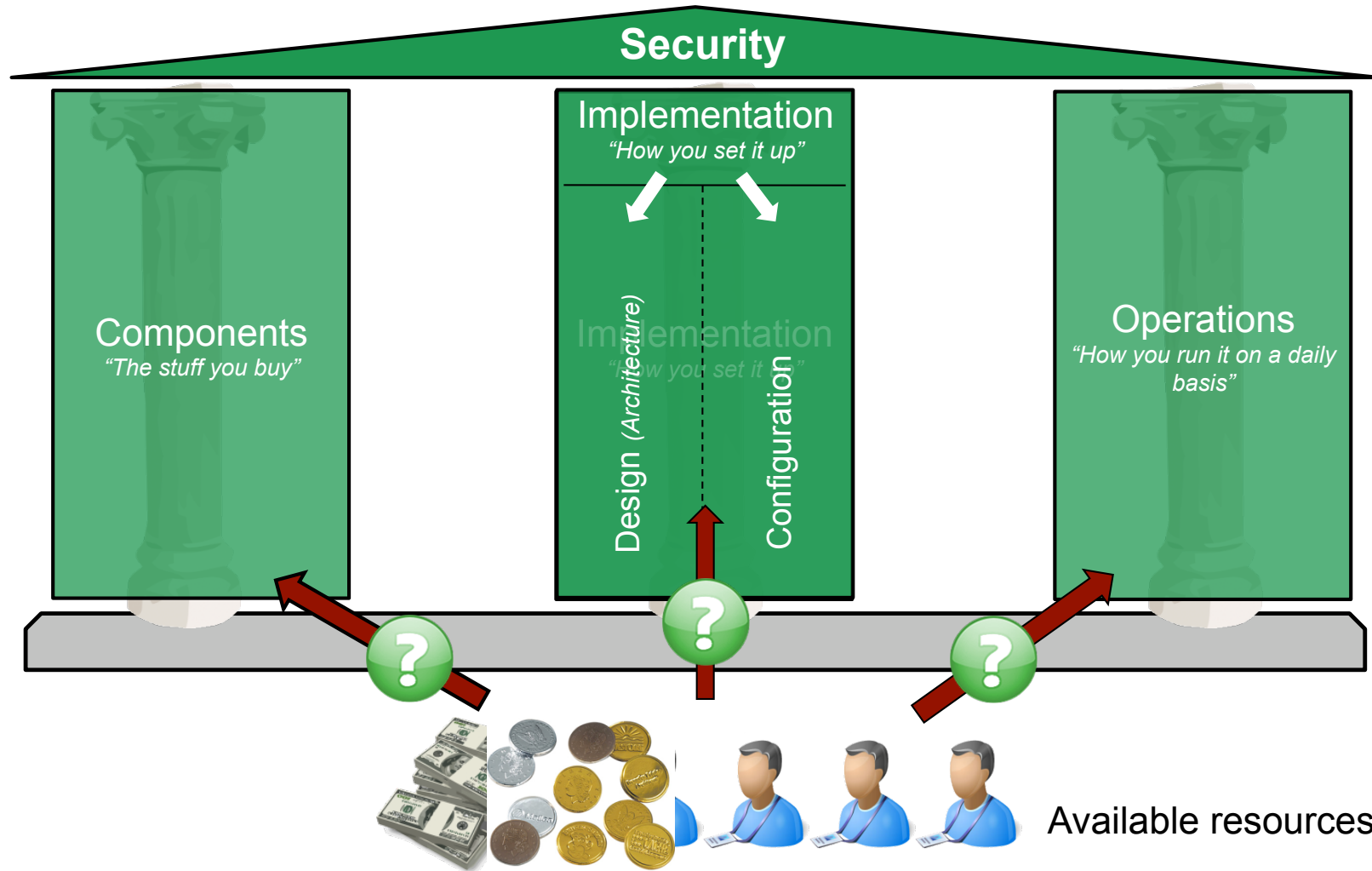
- **Technology**
- **Communication & Tools**
- **Mindset & Approach**

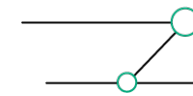


- **The *house of security* & the role of operations**
- **The ongoing change of the threat landscape & subsequent consequences**
- **The evaporation of network based controls**
- **See my *Troopers09* keynote for more on this stuff**

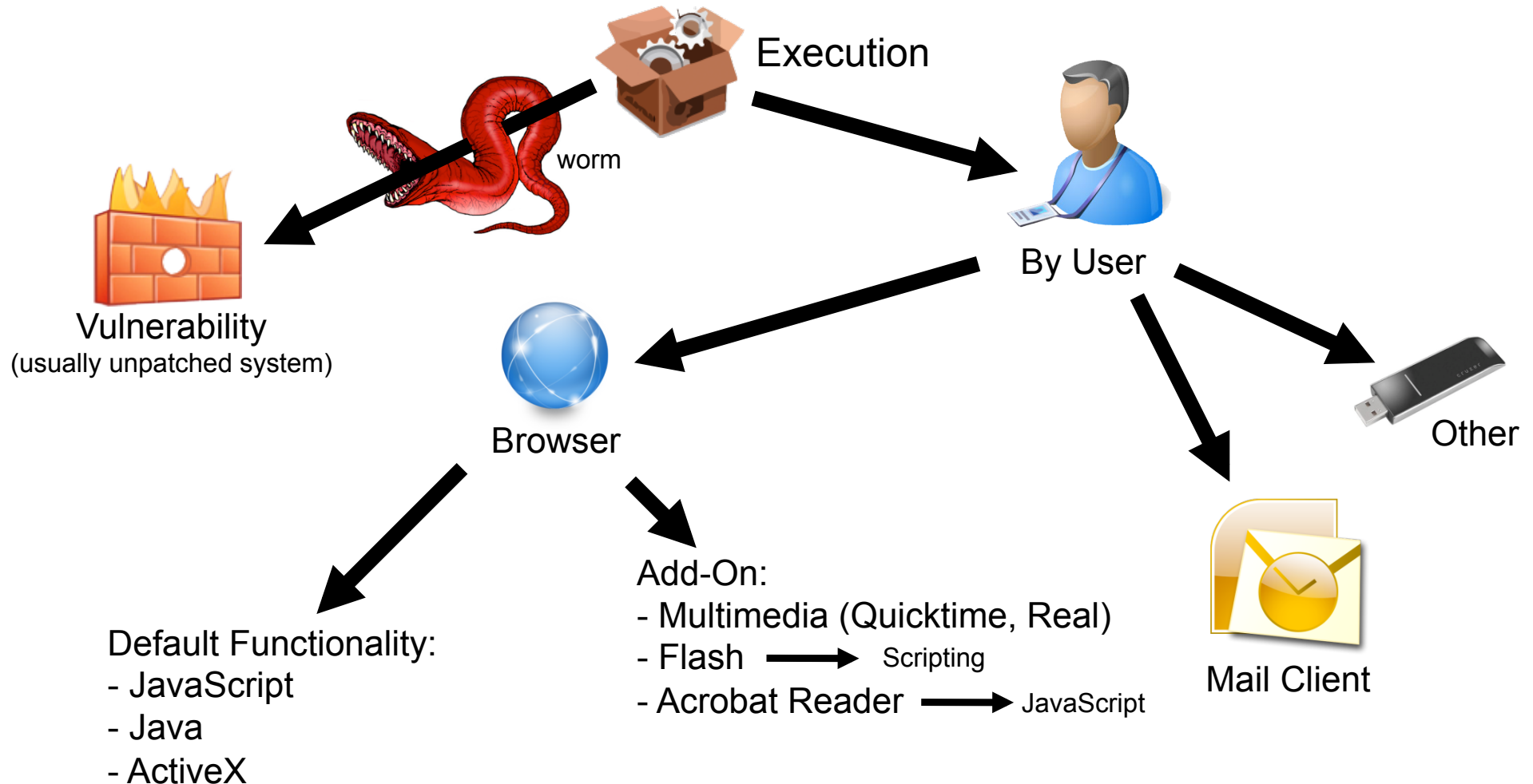


The House of Security

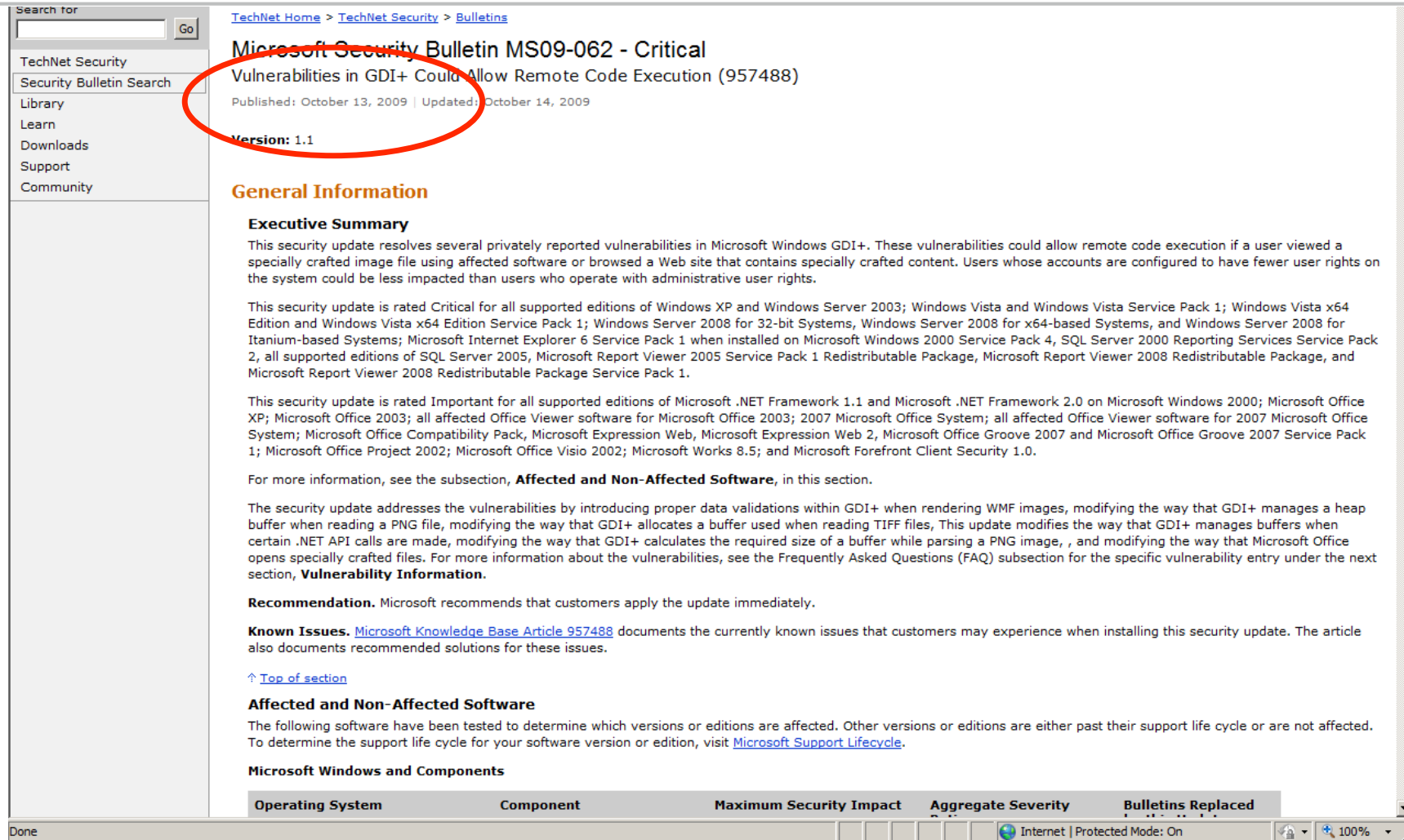




How malicious code gets on system



In the light of recent events...



Search for Go

TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
Community

[TechNet Home](#) > [TechNet Security](#) > [Bulletins](#)

Microsoft Security Bulletin MS09-062 - Critical

Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)

Published: October 13, 2009 | Updated: October 14, 2009

Version: 1.1

General Information

Executive Summary

This security update resolves several privately reported vulnerabilities in Microsoft Windows GDI+. These vulnerabilities could allow remote code execution if a user viewed a specially crafted image file using affected software or browsed a Web site that contains specially crafted content. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This security update is rated Critical for all supported editions of Windows XP and Windows Server 2003; Windows Vista and Windows Vista Service Pack 1; Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1; Windows Server 2008 for 32-bit Systems, Windows Server 2008 for x64-based Systems, and Windows Server 2008 for Itanium-based Systems; Microsoft Internet Explorer 6 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4, SQL Server 2000 Reporting Services Service Pack 2, all supported editions of SQL Server 2005, Microsoft Report Viewer 2005 Service Pack 1 Redistributable Package, Microsoft Report Viewer 2008 Redistributable Package, and Microsoft Report Viewer 2008 Redistributable Package Service Pack 1.

This security update is rated Important for all supported editions of Microsoft .NET Framework 1.1 and Microsoft .NET Framework 2.0 on Microsoft Windows 2000; Microsoft Office XP; Microsoft Office 2003; all affected Office Viewer software for Microsoft Office 2003; 2007 Microsoft Office System; all affected Office Viewer software for 2007 Microsoft Office System; Microsoft Office Compatibility Pack, Microsoft Expression Web, Microsoft Expression Web 2, Microsoft Office Groove 2007 and Microsoft Office Groove 2007 Service Pack 1; Microsoft Office Project 2002; Microsoft Office Visio 2002; Microsoft Works 8.5; and Microsoft Forefront Client Security 1.0.

For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerabilities by introducing proper data validations within GDI+ when rendering WMF images, modifying the way that GDI+ manages a heap buffer when reading a PNG file, modifying the way that GDI+ allocates a buffer used when reading TIFF files, This update modifies the way that GDI+ manages buffers when certain .NET API calls are made, modifying the way that GDI+ calculates the required size of a buffer while parsing a PNG image, , and modifying the way that Microsoft Office opens specially crafted files. For more information about the vulnerabilities, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. [Microsoft Knowledge Base Article 957488](#) documents the currently known issues that customers may experience when installing this security update. The article also documents recommended solutions for these issues.

[↑ Top of section](#)

Affected and Non-Affected Software

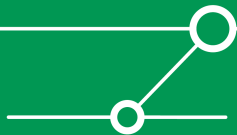
The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit [Microsoft Support Lifecycle](#).

Microsoft Windows and Components

Operating System	Component	Maximum Security Impact	Aggregate Severity	Bulletins Replaced
------------------	-----------	-------------------------	--------------------	--------------------

Done

Internet | Protected Mode: On | 100%



In the light of recent events... II

Adobe Product Security Incident Response Team (PSIRT)

Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT@adobe.com.

Adobe Reader and Acrobat issue

By David Lenoë on October 8, 2009 9:50 AM | [No Comments](#)

Adobe is aware of reports of a critical vulnerability in Adobe Reader and Acrobat 9.1.3 and earlier (CVE-2009-3459) on Windows, Macintosh and UNIX. There are reports that this issue is being exploited in the wild in limited targeted attacks; the exploit targets Adobe Reader and Acrobat 9.1.3 on Windows.

Adobe plans to resolve this issue as part of the [upcoming Adobe Reader and Acrobat quarterly security update](#), scheduled for release on October 13. Adobe Reader and Acrobat 9.1.3 customers with DEP enabled on Windows Vista will be protected from this exploit. Disabling JavaScript also mitigates against this specific exploit, although a variant that [does not rely on JavaScript](#) could be possible. In the meantime, Adobe is also in contact with Antivirus and Security vendors regarding the issue and recommends users keep their anti-virus definitions up to date.

We wish to thank Chia-Ching Fang and the [Information and Communication Security Technology Center](#) for their help with reporting and investigating this issue (CVE-2009-3459).

We will continue to provide updates on this issue via the [Security Advisory section of the Adobe web site](#), as well as the [Adobe PSIRT blog](#).

This posting is provided "AS IS" with no warranties and confers no rights.

Categories: [Security Bulletins and Advisories](#)

Leave a comment

Search

About this Entry

This page contains a single entry by David Lenoë published on October 8, 2009 9:50 AM.

[Potential Photoshop Elements 8.0 issue](#) was the previous entry in this blog.

[Pre-Notification - Quarterly Security Update for Adobe Reader and Acrobat](#) is the next entry in this blog.

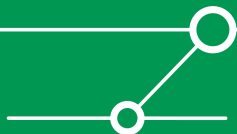
Find recent content on the [main index](#) or look in the [archives](#) to find all content.

Categories

[Security Bulletins and Advisories \(33\)](#)

Monthly Archives

- [October 2009 \(2\)](#)
- [September 2009 \(5\)](#)
- [August 2009 \(3\)](#)
- [July 2009 \(8\)](#)
- [June 2009 \(4\)](#)
- [May 2009 \(2\)](#)
- [April 2009 \(3\)](#)
- [March 2009 \(3\)](#)
- [February 2009 \(3\)](#)
- [December 2008 \(2\)](#)
- [November 2008 \(3\)](#)
- [October 2008 \(3\)](#)
- [September 2008 \(4\)](#)
- [August 2008 \(3\)](#)
- [July 2008 \(1\)](#)
- [June 2008 \(2\)](#)
- [May 2008 \(4\)](#)
- [April 2008 \(2\)](#)
- [March 2008 \(2\)](#)
- [February 2008 \(4\)](#)





The evaporation of Network Based Controls

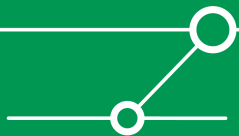
- **Get over it.**
- **In times of “convergence”, VoIP, virtualization, multi-tier monster apps... segmentation & filtering might no more work**
- **Personally, this hurts ;-)**

- **Still, your new**

- Host Hardening
- Encryption

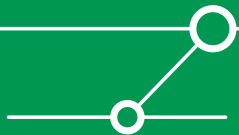


at you? ;-)



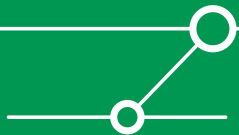
Lessons learned (Really?)

- **Operations is key**
- **Prevention pays**
- **It's the simple things in life...**

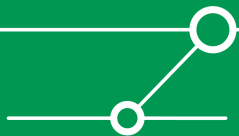


Communication & Tools

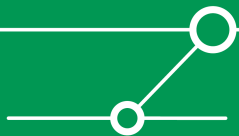
- **Relationships in the organization**
- **Policies**
- **Risk assessment**



Understand who has “the money”



Don't go into fights you can't win.

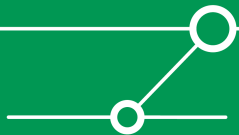


Policies 1

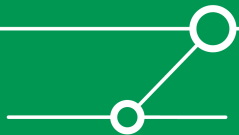
- **In case you've not written them yourself...**



- **Establish line-of-contact to *policy people* in your org**
- **Try to figure out intent if clauses are not clear**



- **In case you write them yourself**
- **Support business**
- **Provide flexibility**
- **Still be distinct & precise! Align with governance model.**
- **It's not a problem having a statement like “apply where appropriate” in your policy as long as**
 - People do not decide about “where appropriate” on their own.
 - They know when and who to ask for guidance.
 - This guidance is provided and there's a governance model.



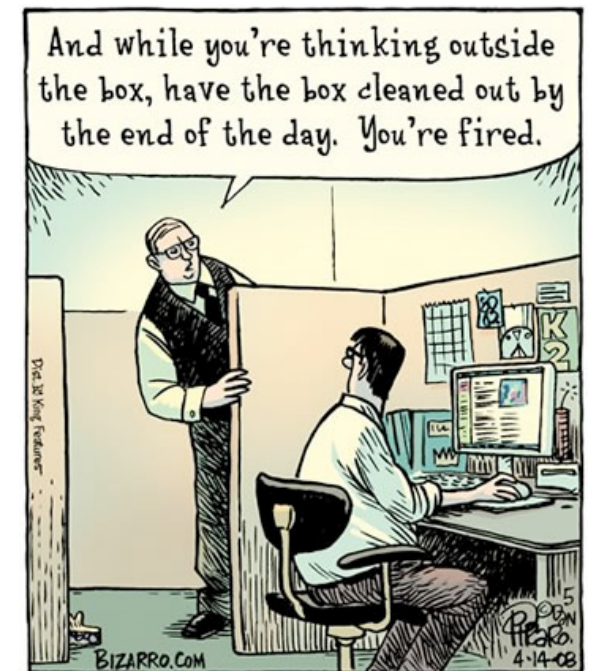
- **Role of “outside world” has changed**

→ Do not think only of “inside corp” (e.g. when writing policies), but always think “outward”

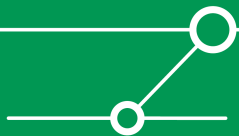
- Main discussion in many environments currently.

How to treat:

- Business partners
- Subsidiaries \$CORP holds 51% of.
 - At least today. Tomorrow it might be 20%...
- External data sources (trading systems, weather forecast etc.).



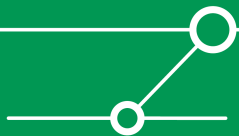
© Dan Piraro



It's all about risk

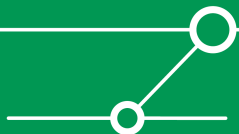
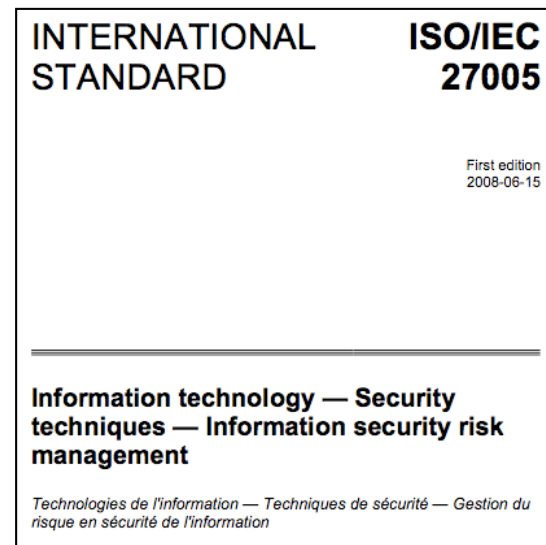


- **You NEED some tools/framework.**
 - Honestly, I can't understand how any CISO can get along without some tools...



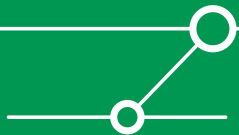
Lessons learned

- Understand who has money & power
- Don't go into fights already-lost
- Get & communicate the role of policies
- USE risk assessment (tools)

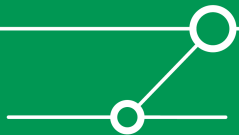


Mindset & Approach

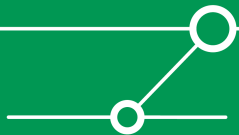
- **Be able to take punches**
- **Risk & Reward**
- **Trust & Control**



Be able to take punches



The concept of reward

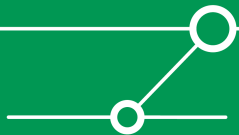


The concept of *reward*

- “Slipping and falling on the ice, for example, is a game for young children, but a potentially fatal accident for an old person. And the probability of such an event is influenced both by a person’s perception of the probability, and by whether they see it as fun or dangerous. For example, because old people see the risk of slipping on an icy road to be high, they take avoiding action, thereby reducing the probability.”
[from: John Adams’s *Risk*]



- But they miss the *fun*, that is the reward.

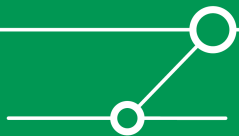


The value of trust

- **Confidence is built on**
 - Trust
 - Control



- **You can't *control* everything**
 - Remember your limited set of resources...
- **So understand where to control... and where to trust...**

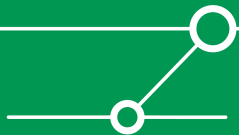
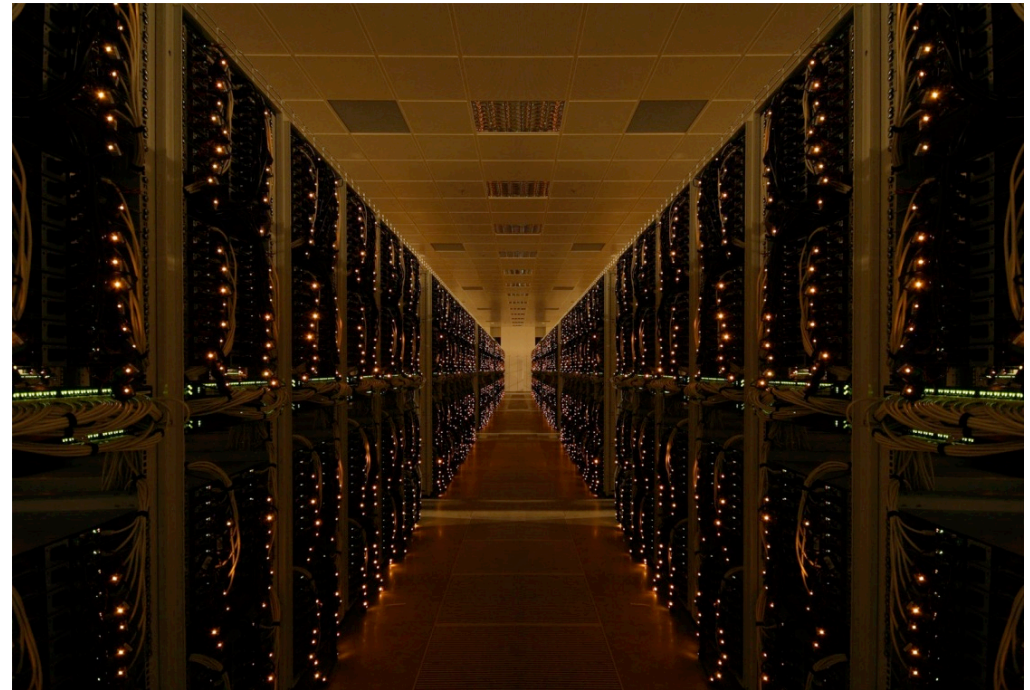


Sometimes you can trust...

Home



Datacenter



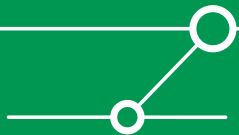
...and sometimes you better control



Home



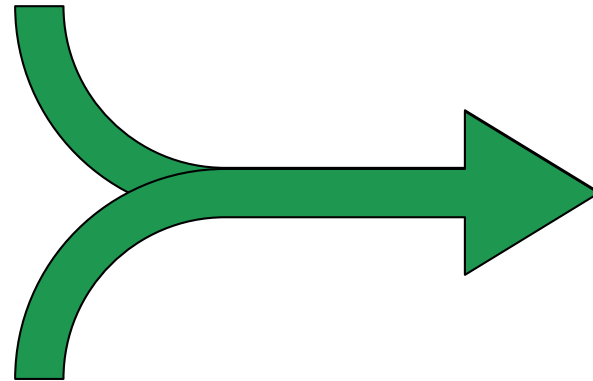
Datacenter



Trust, Control & Confidence



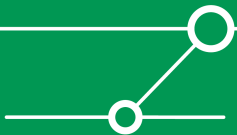
TRUST



CONFIDENCE

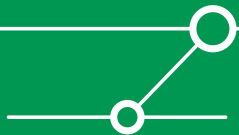


CONTROL



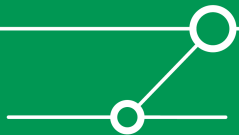
Lessons learned

- **The right mindset is paramount.**
- **There's risk... and reward.**
- **Confidence has two sources...**

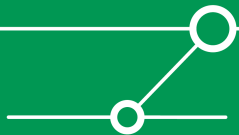


Conclusions

- **Corporate infosec world might be complex and cruel.**
- **YOU can still master it with the right tools & mindset.**
- **And thereby accomplish your future mission...**



Trusted Business Advisor

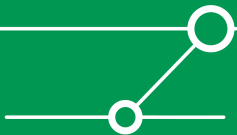


There's never enough time...

THANK YOU...



...for yours!



Photograph Credits - Sources

- **Rocky IV**
 - *Sylvester Stallone, 1985*
- **Rocky Balboa**
 - *Sylvester Stallone, 2006*
- **Indiana Jones Raiders of the Lost Ark**
 - *Steven Spielberg, 1981*
- **Taxi Driver**
 - *Martin Scorsese, 1976*
- **Scarface**
 - *Brian De Palma, 1983*

