AICPA Information Technology Section

2010 AICPA Top Technology Initiatives

Presenter: Dan Schroeder, CPA/CITP
Habif, Arogeti, & Wynne, LLP

Georgia Society of CPAs Annual Convention
June 16, 2010

About the Presenter

Dan Schroeder,
CPA/ CITP, CISA, CISM, CIA

- Partner-in-Charge, Habif, Arogeti,& Wynne LLP ("HA&W") IT Audit & Assurance Services
- SAS 70,SSAE 16, Security and Privacy Trust Services, IT Governance, and other compliance services.
- 20 years of IT advisory and audit experience - focused mainly on financial services, mfg/distribution, and technology service providers.
- Chairperson of AICPA's Information Technology Executive Committee (ITEC)
- Leading author of "IT Considerations for Risk Based Auditing" whitepaper
- Lead development of AICPA IT Audit School.

Agenda

Top Technology Initiatives Background and Results

Results drivers: the Story behind the Story.

Take-Aways

2010 Survey Approach

- **Survey options:** designed by IT Executive Committee with intent to represent the CPA's unique perspective regarding those initiatives they believe will impact financial management and the fulfillment of other fiduciary responsibilities such as safeguarding of business assets, oversight of business performance, and compliance with regulatory requirements.
- **Survey context:** […what are the top technology considerations] that you, your senior management team, or your client may be encountering during the next 12 to 18 months. (example, the audit committee, CEOs, CFOs, CIOs, etc.)
- **20th year of the survey!**
- Managed by the IT Section

Survey results

2010 Top 10 Technology Topics

Relevancy to CFOs, Audit Committees, Audit Partners.

1. Securing data and IT against hacking, viruses, etc.
2. Security precautions for potential data breaches.
3. Internal controls and IT governance effectiveness.
4. Reporting and analytical functions effectiveness (business intelligence, dashboards, etc.)
5. Privacy policies and procedures.

2010 Top 10 Technology Topics

Relevancy to CFOs, Audit Committees, Audit Partners.

6. **IT risk considerations for planning audit and attest engagements.**
7. **Aligning audit procedures to IT risk assessments.**
8. **Adequacy of core accounting and reporting technology.**
9. **Cloud / SaaS –security considerations.**
10. **Cloud / SaaS – reliability considerations.**

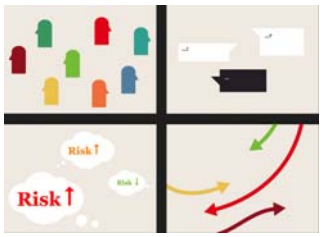
2010 Top Technology Topics
Primary Topics

- **Security**
- **Data Management**
- **Privacy**
- **Cloud computing security, integrity & reliability**
- **Business Intelligence**
- **Risk based approach to:**
  - Management of IT systems
  - IT Auditing and Assurance

HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

The Changing Risk Landscape

- AICPA 2010 Top Technology Topics

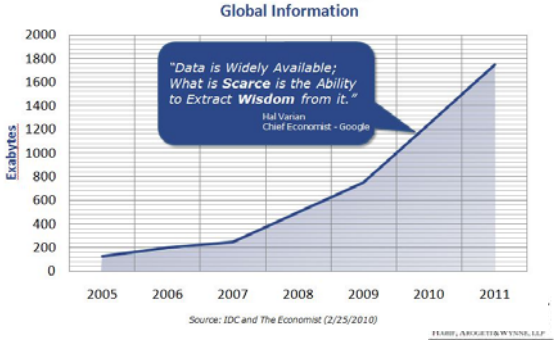


HA&W
Habif, Arogeti & Wynne, LLP
Certified Public Accountants and Business Advisors

Key Risk Concerns: 2010

- Security
- Data Management
- Privacy
- Cloud Computing

The Data Deluge



Data proliferation is key driver of security and privacy risks

- Do you really know what data your company has, where it is, how it is protected?

Legal Regulations

- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act
- Red Flag Rule
- HITECH
- Children's Online Privacy Protection Act
- Drivers License Information Protection
- State information security breach notification requirements
- Massachusetts Information Security Protection Act

For Financial, Health and other Personal Information that can be used for identify theft, electronic data carries greater risk of liability than paper

Legal Regulations

- Generally, the notification obligations under HITECH and State laws requires:
  - any business that owns, licenses or maintains computerized data
  - to disclose any breach of the security of its systems following discovery or notification of the breach in the security of the data
  - if unencrypted personal information of a state resident was, or is reasonably believed to have been, acquired by an unauthorized person
  - Notice required to be delivered to each affected resident

Data increasingly source of regulatory and reputation risk

- Personal information – Individual's first name or initial and last name, in combination with one or more additional data elements such as:
  - Personal health information, social security number, driver's license number, state identification card number, or an account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- **330 million records** containing personal identity-related information have been involved in data breaches since 2005

Security Threats: from cyber vandalism to cyber thieves

- **Phishing** – the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into giving private information that will be used for theft.
  - Social networks increasingly targeted by phishing
- **Pharming** – a hacker's attack aiming to redirect a website's traffic to another bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in software.

Phishing, Malware and ACH Fraud

- Online fraud – 2009 est. $559M, double 2008
- Spearphishing: targeted email; e.g., to controller, or other executive, requesting they click on link for some apparently official purpose. Link installs Trojan malware, usually for keystroke logging, often to identify banking credentials.
- Banking Trojan malware:
  - Readily for sale on Internet.
  - Estimated to be in 88% of Fortune 500

NETWORKWORLD http://www.networkworld.com/news/2010/031110-zeus-botnet.html

ZeuS botnet code keeps getting better... for criminals

$10,000 will buy a ZeuS module that takes complete control of a compromised PC

By Ellen Messmer, Network World
March 11, 2010 04:19 PM ET

Share/Email | Tweet This | 29 Comments | Print | Newsletter Sign-Up

New capabilities are strengthening the ZeuS botnet, which criminals use to steal financial credentials and execute unauthorized transactions in online banking, automated clearing house (ACH) networks and payroll systems. The latest version of this cybercrime toolkit, which starts at about $3,000, offers a $10,000 module that can let attackers completely take control of a compromised PC.

America's 10 most wanted botnets

Zeus v.1.3.4.x (code changes are always underway by the author and owner, who is believed to be one individual in Eastern Europe) has integrated a powerful remote-control function into the botnet so that the attacker can now "take complete control of the person's PC," says Don Jackson, director of threat intelligence at SecureWorks, which released an in-depth report on ZeuS this week.

This new ZeuS feature, which was picked up from an older public-domain project from AT&T Bell Labs known as "Virtual Network Computing," gives ZeuS the kind of remote-control capability that might be found in a legitimate product like GoToMyPC, Jackson says.

&W Wynne, LLP

Cloud Computing expanding risk landscape

- **SaaS** – single application, multi-tenant architecture; e.g., Salesforce.com, Google apps
- **Utility Computing** – storage and virtual servers.
- **Web Services** –e.g., Google Maps, ADP payroll, USPS, etc.
- **PaaS** – development environments as a service; e.g., Intuit Partner Platform
- **MSP** – Managed Service Provider – application exposed to hosted IT functionality, rather than to users; e.g., SecureWorks, and Postini.
- **Service Commerce Platforms** – e.g., expense management systems, purchasing, e.g., Reardon Commerce, ARIBA

HA&W Habif, Arogeti & Wynne, LLP Certified Public Accountants and Business Advisors

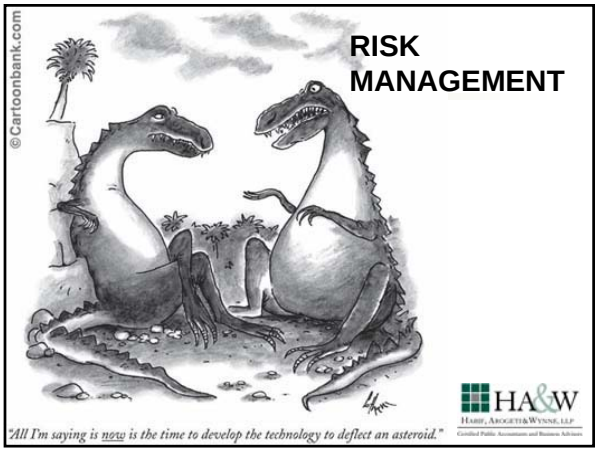
AICPA 2010 Top Technology Topics

LEVERAGING NEW(ER) TECHNOLOGIES

HA&W Habif, Arogeti & Wynne, LLP Certified Public Accountants and Business Advisors

Leveraging technology

- Cloud computing
- Business Intelligence (Enterprise Performance Management)
- Systems upgrade / replacement



Question of "Trust / Reliance" Key Theme in Survey

6. IT risk considerations for planning audit and attest engagements.
7. Aligning audit procedures to IT risk assessments.
9. Cloud / SaaS –security considerations
10. Cloud / SaaS – reliability considerations

HOW DOES AN AUDITOR (OR A USER) OF A SYSTEM KNOW IT IS TRUSTWORTHY?

IS THERE A ONE-SIZED FITS ALL APPROACH?

IT Creates Many Types of Risks

- Financial risks – for Auditors – "ICFR"
- Security Risks
- Confidentiality
- Availability
- Processing Integrity
- Privacy

Compliance and Operational Risks

Risk-Based Approach to Assurance & Audit

- Whether provider or user of IT services:
  - Understand role of IT
  - Understand Inherent Risks
  - Understand if mitigating controls are adequate
  - Improve controls as needed
  - Audit / assurance reporting (if needed)

Service Provider Risk Management: (Cloud / SaaS)

- No one-size fits all approach
- SAS 70 being replaced by SSAE 16

AICPA Assessment and Attestation Reporting Options for different types of service provider risk

Type of Risk	Attestation Controls Guidance
• Financial (ICFR)	SSAE 16
• Security • Confidentiality • Availability • Processing Integrity • Privacy – *Generally Accepted Privacy Principles ("GAPP")*	AICPA Trust Services Principles & Criteria

AICPA 2010 Top Technology Topics

TOP TAKE-AWAYS FOR TRUSTED BUSINESS ADVISORS

Data Management: new management discipline needed

- Know what data your business collects, where it resides, who accesses it, how it is shared, purged, etc.
- Understand applicable regulations.
- Limit collection and storage of identity related data to that which is absolutely essential.
- Assess data management risk and develop commensurate risk management program involving policies, procedures, system controls, and insurance.
  - Policies and procedures pertain to Classification, Access and security, Retention, and Disclosure

Security considerations

- Always run strong antivirus software that includes browsing protection that can automatically detect suspicious sites and malicious code.
- When accessing sensitive websites (e.g., banking), look for site keys or other advanced forms of authentication (e.g., biometrics) to reduce phishing risk.
- Restrict use of administrative rights on end user devices – if not possible, monitor for presence of unauthorized functions.
- Extend security to handheld devices and smartphones: passcodes and screen locks after idle time, and capability to remotely wipe the device.
- Stay current on patches and updates.

Additional Controls to Prevent Banking Fraud

- Talk to your bank and understand the security controls that are available with your online banking system.
- Use a separate computer for online banking that is segmented from rest of the network.
- The computer should have internet access only to the banking website and nothing else.

The Human Firewall

- A good *human firewall employee is one who filters good security practices and rejects any others—much like a network firewall only allows authorized traffic and rejects any other*
- The only way to build a good human firewall is to raise people's awareness; to teach them good habits, to make them recognize bad practices and change them into good practices
- Your cyber security is only as good as the people who manage it and those who use it

Source: Patrick Gray, CISCO,
Atlanta, GA 2010 Secureworld Conference

Education is key

- Few executives grasp the case for investing in safeguards against hackers, worms, and the like.
- Education starts at the top and works its way down the food chain throughout the entire business.
- Employees must understand that it is not ***their computer.***

Source: Patrick Gray, CICSO,
Atlanta, GA 2010 Secureworld Conference

Recap: 2010 Top 10 Technology Topics

Relevancy to CFOs, Audit Committees, Audit Partners.

1. Securing data and IT against hacking, viruses, etc.
2. Security precautions for potential data breaches.
3. Internal controls and IT governance effectiveness.
4. Reporting and analytical functions effectiveness (business intelligence, dashboards, etc.)
5. Privacy policies and procedures.
6. IT risk considerations for planning audit and attest engagements.
7. Aligning audit procedures to IT risk assessments.
8. Adequacy of core accounting and reporting technology.
9. Cloud / SaaS –security considerations.
10. Cloud / SaaS – reliability considerations.

Contact Info.

Dan Schroeder
dan.schroeder@hawcpa.com
770-353-8379

AICPA IT Section Member Benefits

- Discounts on Educational programs, such as AICPA TECH Conference and IT Audit School program
- Discounts on valuable software and tools, including IDEA products and training sessions with Audimation Services
- Free monthly web seminars on topics critical to CPAs (plus an opportunity for CPE discounts!)
- Valuable technology content, including discussion papers, studies & practice aids
- Communications, including electronic newsletters, podcasts, featured articles, profiles and news about the profession and the IT Community
- Networking groups and IT Community events at TECH+ conference

AICPA CITP Credential holder benefits

IT Section membership, plus:

- Differentiation from CPAs and other technology and financial management professionals
- Customizable marketing materials, including targeted brochures that highlight your ability to leverage technology for real business results
- CITP Networking Groups
- Additional discounts, including $125 discount on conference registration to TECH+!

To find out more about the IT Section membership or the Certified Information Technology Professional (CITP) Credential, please go to http://infotech.aicpa.org for more details.

More Information

- Additional Top Technology Initiatives information is available on the IT Center Website:
- www.aicpa.org/TopTech

- For further information, e-mail ITinfo@aicpa.org or call 888-777-7077, option 4 from 9:00am-6:00pm ET.

- Subscribe to the Top Technology Initiatives Podcast!
- Visit http://toptechinitiatives.podomatic.com/