

# What every Financial Professional Needs to Know about Cyber Security

Presenters – AFP Winter Seminar

12/9/2011

David Sturdivant, Treasury Management Manager  
Mark Brown, Information Security Officer



# Cyber Security – Compliance it's the Law

Recognize these acronyms? If not, its time to brush-up. <sup>1</sup>

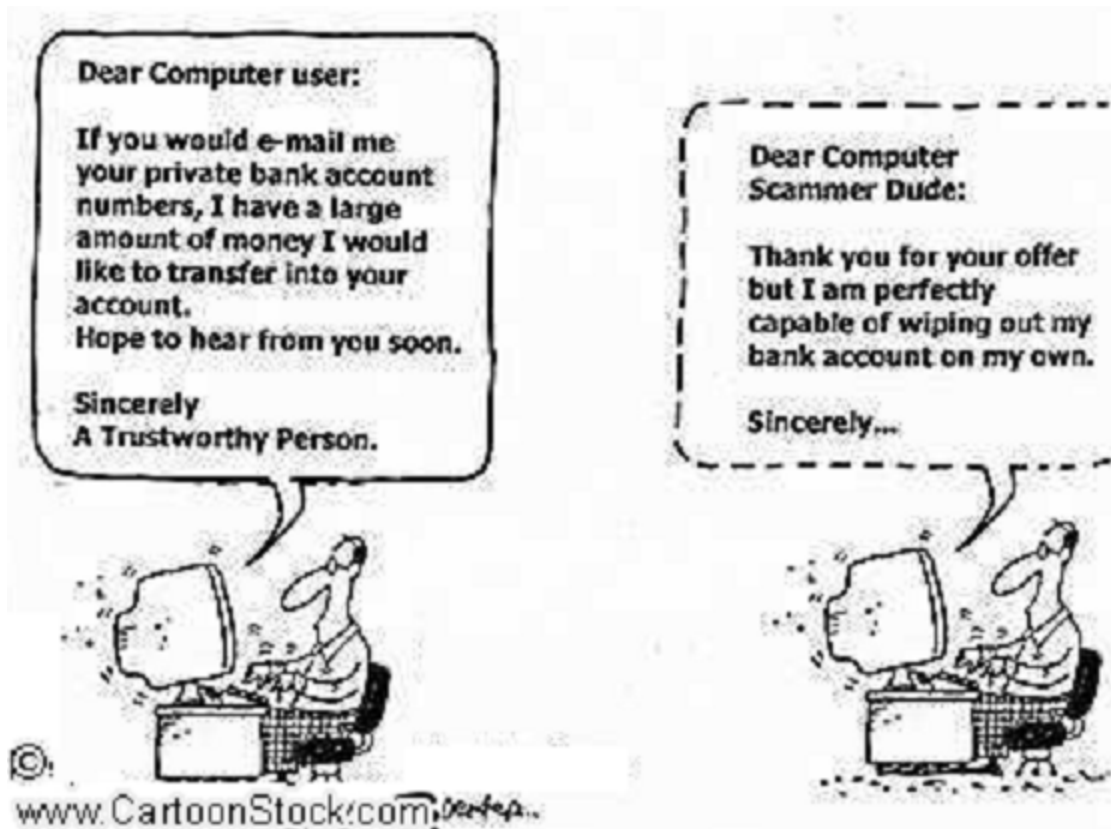
Cyber-security standards and practices are an increasing part of your companies regulatory/audit landscape.

---

- **SOX** and recently changed **SEC guidelines** <sup>2</sup> for public firms
- **GLBA**, and **updated FINRA (social media)**<sup>3</sup> and **FFIEC** guidance<sup>4</sup> for financial firms
- **HIPAA** and **HITECH** for healthcare firms and their business partners
- Changed **PCI**<sup>5</sup> standards for those storing, transferring, or processing credit and debit card transaction data.
- In addition to Federal regulations, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted **privacy regulations**<sup>6</sup> requiring that companies and/or state agencies disclose to consumers security breaches involving personal information.
- And other cyber security and privacy regulations including international standards (**EU Data Protection Act, Safe Harbor Act**, etc)

# Cyber Security – it's also your Bottom Line

Accidents, Data Breaches, and Cyber Crime, it could happen to you too.



# Your Bottom Line (cont.)

- [“Sony, which suffered multiple data breaches](#) across its online entertainment sites in April, initially estimated clean-up costs at least \$171 million. [It had to warn investors](#) that the breach, which affected 101 million users and ranks as one of the largest to date, would have a sharp impact on its fiscal 2011 year. One major cost: the free year of identity-theft monitoring that the company is offering PlayStation Network and Qriocity users whose names, addresses, birth dates, purchase histories and online identifications were stolen.”
- “The repercussions of an 18-month hack that began in July 2005 cost [TJX](#), parent company of clothing chains TJ Maxx and Marshalls, \$256 million. The retailer saw \$118 million erased from its 2007 second-quarter profits to deal with the attack, during which hackers made off with 45.6 million credit and debit card numbers.”
- “The [Hannaford chain](#) likely will see in its legal expenses soar after a recent federal appeals court decision related to a 2007 data breach. [The ruling](#) allows a class-action lawsuit against Hannaford to proceed. Victims are seeking compensation for the measures they took to protect themselves from identity theft and fraud after perpetrators pilfered 4.2 million credit and debit card numbers.”<sup>7</sup>

# Cyber Crime – Its Big Business and Growing

- [“Cybercrime Losses More Than Drug Profits Says Symantec”](#) (9/2011)



# Financial Pro's New Role in Cyber Security ...

Its not just for “your IT geeks” to understand anymore.

1. Be sure internal audits include compliance for all areas applicable to your firm/clients. Ignorance is not bliss when it comes back to bite you and/or regulators and external audit teams come onsite.

No internal IT audit team? Request periodic IT security risk reports.

You should include:

- updates to your security policies and information security program
- all IT security testing activities/failures
- vendor management security and contractual reviews
- all internal or external incidents and management actions to resolve, including projected costs (see SEC footnote <sup>2</sup>)
- projected changes to compliance/audit status based on new company activities, client changes, etc. (consider SOX, PCI, HIPAA, FINRA, etc)

# Financial Pro's New Role (cont.)

2. Have IT adopt a risk-based approach to security expenditure requests. Adapt the firm's Enterprise Wide Risk Model to better understand dimensions of IT risk and projected future budget needs.

Key – cyber risks should be prioritized based on work (mitigants) already protecting your firm. Fewer mitigants and higher risk, expect higher \$\$\$.

3. While IT has a large role to play in ensuring your organization's information is secure (patching, monitoring, etc) ... so do you!
  - consider the CFO's workstation compromised before SEC filing dates due to malware from a targeted spear phishing message
  - consider media consequences of a public data breach. See [privacyrights.org/databreach](https://www.privacyrights.org/databreach). Breach costs avg \$214/record.<sup>8</sup>
  - review your treasury management practices to ensure they include security procedures like secure token usage or dual authentication

# Firewall, intrusion detection and antivirus, check!

Your IT team is fighting a new breed of criminal, and need new tools.  
Consider asking:

1. how up to date is our server/workstation patching process?  
If more than 30 days since latest updates, its probably too long.  
Many vendors constantly update their 3<sup>rd</sup> party software and plug-ins.

solutions – strong 3<sup>rd</sup> party patching scanners and tools

2. are internal endpoints/workstations are adequately protected from  
“zero-day” threats (no vendor patch/signature exists)?

solutions – in addition to latest antivirus engines, consider application whitelisting and botnet detection services

## Best Practice Solutions (cont.)

3. Are suspicious network activities being logged, reported, and managed to resolution on a daily basis?

solutions – advanced logging, detection and aggregation tools like Security Incident Event Management tools (SIEM) can help

4. If you offer financial services to clients through online sites (ACH, wire) etc. have you reviewed the updated FFIEC guidance<sup>4</sup> (in force 1/1/2012)?

Key notes:

- ensure your logins to high-risk financial sites include multi-factor authentication
- ensure you are monitoring for suspicious activity
- educate clients on Reg E and risks of conducting financial activities online
- consider additional add-ons and mitigants for safe client browsing

# Best Practice Solutions (cont.)

5. If you are a financial services firm, are we considering letting associates access to social media sites for work purposes?

Key notes:

- FINRA regulation 11-39 specifically addresses what must be logged and monitored, and archived regarding these types of interactions.
- even if your firm isn't in the financial industry FINRA 11-39 is being viewed as "best practice" for managing social media interactions.

6. What does our internal (associate) and external (client) overall security awareness program? Does it include specific examples and education around malware prevention and spear-phishing? How is it tested?

- solutions – your best dollars are spent on education of associates and clients. Spear phishing is prevalent and growing. Services exist to help test your associates on their ability to detect fraudulent email.

# Top 5 Things You Can Do To Improve Your Overall Operational Security

1. Store critical data centrally (on network folders, **not** on C: or USB drives, etc.)
2. Secure critical data physically (put locks on the doors to your servers)
3. Cross-cut shred all sensitive documents
4. Require segregation of duties, dual authentication for sensitive financial transactions
5. Make passwords hard to guess, but easier to remember with substitute characters and phrases. Consider making them longer. Examples: @ for "A", ! For "I", 3 for "E", etc.

# Additional Operational Security Tips

- Control your check stock (Advanced copiers make it easier to duplicate checks)
- Set internal \$ limits for individual check writing authority
- Utilize Positive Pay service
- Review bank statement activity
- Monitor account balances
- Build in dual controls or review
- Hire the right people

# Fraud Control Helpful Links

- Survey conducted in 2010 by the Deloitte Forensic Center. 277 senior executives responded when asked to rate their company's effectiveness in key areas of fraud control.

[http://www.deloitte.com/view/en\\_US/us/Services/Financial-Advisory-Services/Forensic-Center/86b3b3d77f1fb110VgnVCM100000ba42f00aRCRD.htm](http://www.deloitte.com/view/en_US/us/Services/Financial-Advisory-Services/Forensic-Center/86b3b3d77f1fb110VgnVCM100000ba42f00aRCRD.htm)

- "Managing the Business Risk of Fraud: A Practical Guide" – pdf document on Association of Certified Fraud Examiners web site. Principles for establishing effective fraud risk management, regardless of the type or size of an organization, are outlined in the guide.

<http://www.acfe.com/guidancepaper/guidancepaper.asp>

# Footnotes and Appendix

1. [“The Security Laws, Regulations and Guidelines Directory”](#). (CSO Online)
2. [“A Reason to Revisit Your Cybersecurity Risk”](#)  
(CFO.com, Sarah Johnson, 11/3/2011)
3. **FINRA** - [“Regulatory Notice 11-39, Guidance on Social Networking Websites and Business Communications”](#). (FINRA.org, 8/2011)
4. **FFIEC.gov** - [2005 Authentication in an Internet Banking Environment  
2011 Supplement to Authentication in an Internet Banking Environment](#)
5. [PCI DSS v2.0](#). (pcisecuritystandards.org, 10/28/2010)
6. [“Standing In The Breach - State Law Requirements When a Customer Data Breach Occurs”](#). (americanbar.org, Shane B. Hansen and Jordan Paterra)

# Footnotes and Appendix (cont.)

7. ["The CFO's Role in the Data Breach War"](#)  
(PCWorld.com, [Fred O'Connor](#), 11/23/2011)
  
8. \$214 Per Record Data Breach Cost. ["Cost of a Data Breach Climbs Higher"](#)  
(ponemon.org, 3/8/2011)

# Glossary – your Security Lexicon

Its not just your father's viruses anymore ...

- **Key logger/ spyware** – malware collecting keystrokes of victims, sending back to remote site for collection/analysis.
- **Malware** – group of “bad” software designed to intrude, “sniff”, capture and/or exploit your data.
- **Phishing** – web sites, email, text messages, and phone calls (skillfully) assuming someone else's identity in order to obtain your information.
- **Rootkit** – malware designed to stealthily overtake a system's core process functions, giving it “root” or full system control.
- **Trojan** – malware posing as legitimate software.
- **Worm** – malware which replicates/morphs itself. Relies on stealth security to remain undetected. (e.g. polymorphic virus)
- **Zombie** – a machine that is remotely “owned” due to presence of malware. Used by hackers to disguise attacks and cause mass disruption simultaneously using a “zombie net”.

# Laws and Regulations cont.

1. **CA SB 1386** – held commonly as a privacy standard for the rest of the US, California’s privacy regulation and breach notification requirements will likely guide a similar national standard in the future.
2. **FFIEC - Federal Financial Institutions Examination Council**, is a formal interagency body of the US government empowered to prescribe uniform principles, standards, and report forms for financial institution exams.
3. **GLBA** – Gramm-Leach Bliley Act. Congressional bill defines security and IT operations standards for financial institutions.
4. **HIPAA** - Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996 governs security of personal health data.
5. **PCI** – Payment Card Industry standard. Defines security and encryption standards for all debit/credit card data.
6. **SOX** – Sarbanes Oxley. Defines security policies and procedures for publicly traded companies.

# Questions and Contact Information

Questions?

Feel free to contact us if we can help further.

- David Sturdivant, Treasury Management Manager  
Pinnacle Financial Partners  
email – [david.sturdivant@pnfp.com](mailto:david.sturdivant@pnfp.com), wk – 615.744.3726
- Mark Brown, ISO  
Pinnacle Financial Partners  
email - [mark.brown@pnfp.com](mailto:mark.brown@pnfp.com), wk – 615.690.1401

# Bios – David Sturdivant



**David Sturdivant**  
Treasury Management Manager

**David Sturdivant** serves as manager of Pinnacle's Treasury Management services.

Sturdivant began his financial services career in 1988. Before coming to Pinnacle prior roles were with SunTrust Bank in its cash management sales and consulting group and as an account analysis product manager at NationsBank. He was also cash manager at Service Merchandise Co., Inc.

Sturdivant is a graduate of Goodpasture Christian School and earned a bachelor's degree in business administration from the University of Mississippi. He is a certified cash manager.

He is based at Pinnacle's downtown Nashville office at Pinnacle at Symphony Place.

# Bios – Mark Brown



**Mark Brown**  
Information Security Officer

**Mark Brown** serves as Information Security Officer for Pinnacle Financial Partner's Risk and Performance Management team, responsible for the firm's enterprise security program.

Brown began his IT career in 1994 as a consultant with Fortune 500 firm Electronic Data Systems (EDS now HP). Before coming to Pinnacle, his prior roles were with Spheris as Information Security Manager for their worldwide information security program. He also held roles at CIGNA Government Services and Oak Ridge National Laboratory.

The former President of the Middle TN Information Systems Security Association chapter (2009-2010), Brown earned a bachelor's degree in Management Information Systems from Tennessee Technological University and an MBA from the Massey School of Business at Belmont University. He has earned his CISSP, CISM, CISA, and Security+ credentials.

He is based at Pinnacle's downtown Nashville office at Pinnacle at Symphony Place.