Deloitte.

But what if it did happen…

Understanding your cyber threat awareness

Daniel Gabriel
Deloitte & Touche LLP
July 30, 2013

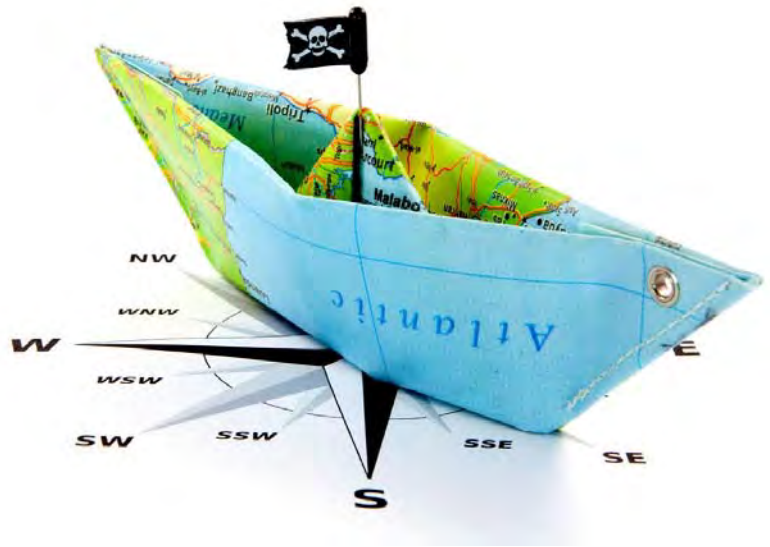
Introduction

Daniel Gabriel, Senior Manager, Security & Privacy
Deloitte & Touche LLP

Daniel has over ten years of experience providing enterprise resource planning (ERP) security and control implementation and review services across numerous industry sectors including State and Local Government. He has extensive project management and hands-on experience in global security solution implementations, redesigns, segregation of duties (SOD) analysis, and Governance, Risk and Compliance (GRC) initiatives. Daniel has spent the last few years focused on providing IRS Publication 1075 services to a number of State agencies. In addition to driving ERP security and control solutions, Daniel has experience leading security information and event management (SIEM), identity and access management (IAM), and data loss prevention and monitoring solutions for many Deloitte clients.

Objectives

- ❑ Understand common misconceptions Agency's face when dealing with potential cyber threats
- ❑ Learn what steps to take in the event a beach occurs
- ❑ Gain insights into a tested method of approaching security threats in a cyber world



Topics

Myths & reality

A breach is on the horizon

Preparing for the inevitable

Questions

Myths & reality

We have a firewall, so we’re good… right?

Myths

Misperceptions about an organization's security posture run rampant in both public and private industries

Myth #1	"Our people would never do that <insert malicious or accidental activity here> they know better"
Myth #2	"Policies and procedures will take care of it"
Myth #3	"We've fortified our environment with <insert protection mechanism here> and now we're covered"
Myth #4	"We have encryption, everything is protected"
Myth #5	"It won't happen at our Agency"

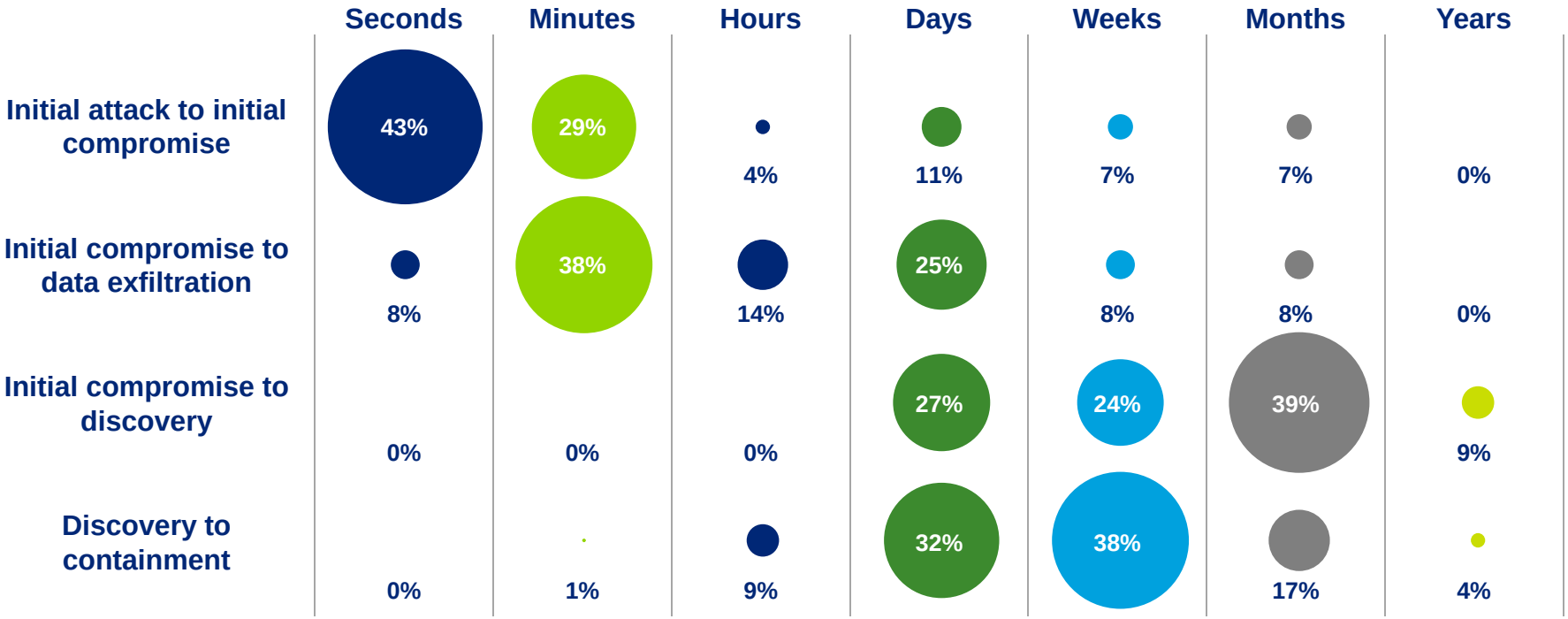
“Since 2007, identity theft passed drug trafficking as the number one crime in the nation.” – *US Department of Justice*

Reality – the advancing threat

The odds aren't in your favor

Attackers have a limitless number of attempts to compromise an Agency's defenses, but it only takes a single weakness.

It is an unfair game, but you may be able to prevent or significantly limit damage by efficiently identifying and dealing with instances of compromise.

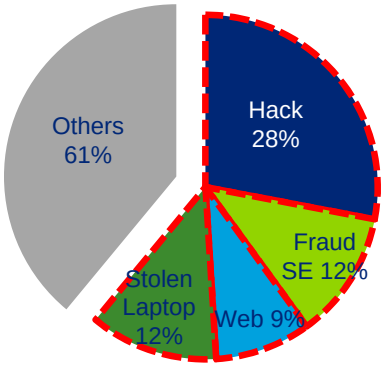


Source: Verizon 2012 Data Breach Investigations Report

This isn't just a private sector problem

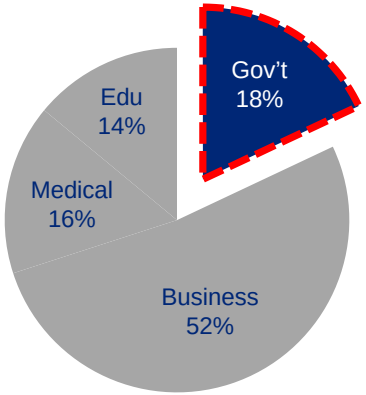
Which organizations have concentrated volumes of personal identifiable information (PII) combined with heavy resource constraints?

Incidents by Breach



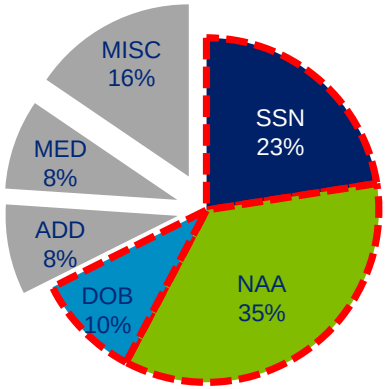
Attacks are trending toward greater sophistication

Incidents by Business Type



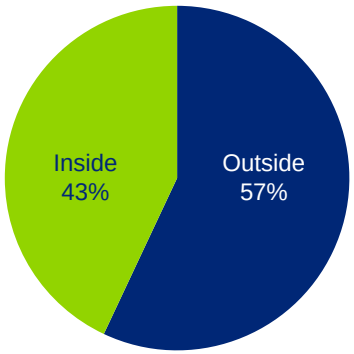
There's a rise in public sector breaches

Incidents by Data Type



States are the best sources of loosely protected PII

Incidents by Vector



Insiders continue to rise as a viable source of threats

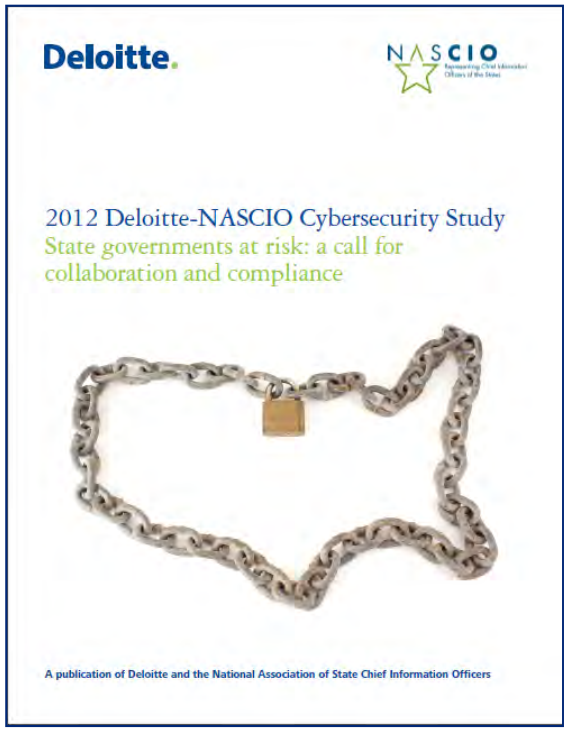
The threat of a breach is real and here to stay

Source: http://datalossdb.org/statistics

2012 Deloitte-NASCIO Cybersecurity Study

The changing face of external breaches (2010 vs. 2012)

	2010	2012	Change
Malicious software	68%	58%	↓
Web	55%	30%	↓
Hackers	45%	30%	↓
Physical attack, such as stolen laptop	36%	20%	↓
Foreign state-sponsored espionage	6%	12%	↑
External financial fraud	4%	12%	↑



Source: 2012 Deloitte-NASCIO Cybersecurity Study

Emerging cybercrime and state-sponsored threats will require a strong response from states.

Looking at the numbers

Year on year upward trending

94 million

The number of Americans' files in which personal information has been exposed to potential identity theft through data breaches at government agencies since 2009.

680%

The increase in significant cybersecurity threats against U.S. government systems from 2006 to 2011.

Source: 2012 Deloitte-NASCIO Cybersecurity Study

A window into the C-suite's cyber concerns

Confidence doesn't run high on cyber-preparedness

92%	State officials feel cybersecurity is very important for the State
50%	CISOs manage a team of only one to five cybersecurity professionals
Only 14%	CISOs feel that they receive appropriate executive commitment and adequate funding for cybersecurity
70%	State CISOs have reported a breach
Only 24%	CISOs are very confident in protecting State's assets against external threats
Only 20%	CISOs feel that staff have the required cybersecurity competency
86%	CISOs indicate "Lack of sufficient funding" is the key barrier to address cybersecurity
82%	CISOs feel "phishing and pharming" as their top cybersecurity threat

An urgent call to execute on a robust cybersecurity strategy, with strong governance and compliance monitoring measures

Source: 2012 Deloitte-NASCIO Cybersecurity Study

A breach is on the horizon

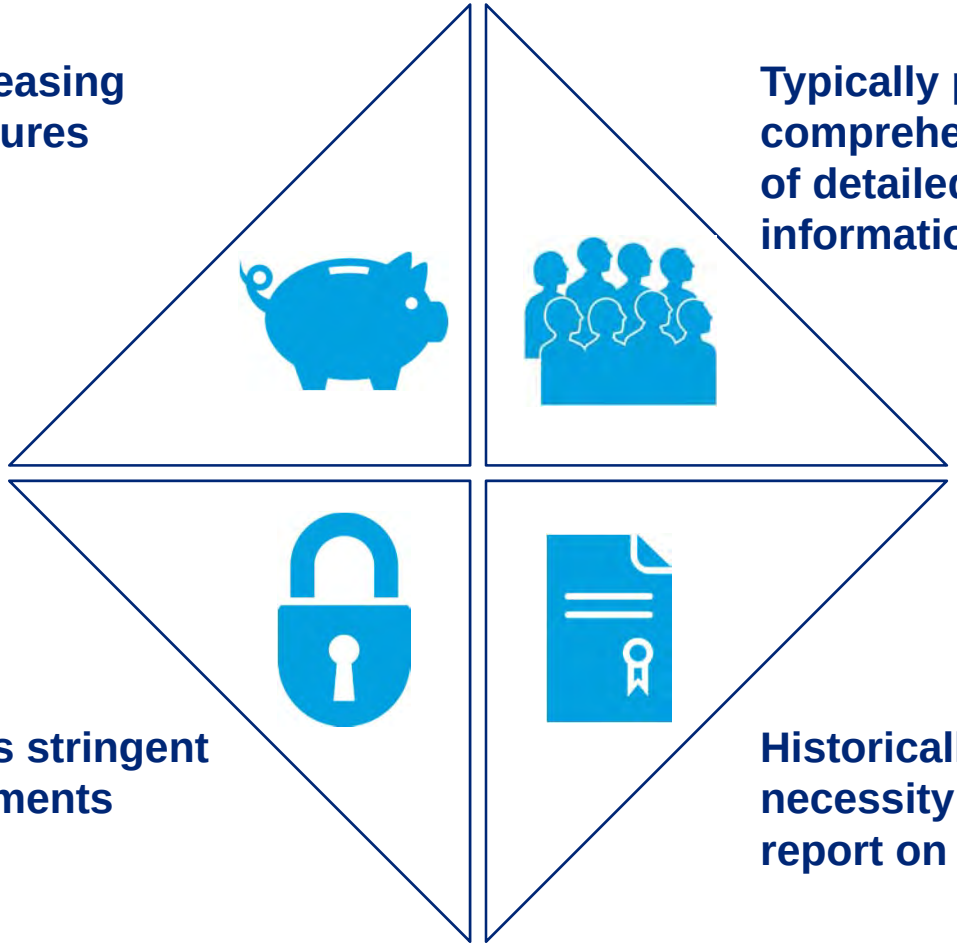
How will the Agency react?

Why us?

Driving forces behind an increase in State focused attacks

Continually increasing budgetary pressures

Typically possess the most comprehensive collection of detailed citizen information



Traditionally less stringent security requirements

Historically a lack of necessity to assess and report on security posture

One thing to remember…

…it could eventually happen to you.

Is your Agency prepared?

Costly implications

Total costs are not easily quantified

Financial Implications

- Average cost to the organization is estimated at **$194 per compromised record**[11] This doesn't include the intangible costs such as goodwill

Regulatory Risks

- States depend heavily on the Federal Tax Information (FTI) interfaces from the IRS. Disruption to this may **impact the ability** of agencies to assess and **collect taxes**
- Civil/criminal **legal action** (class action lawsuits)

Operational Risks

- Potential **decline in voluntary tax filing/compliance** – even if temporary, will have a significant impact
- **Re-allocation of staff** time and resources to **support breach response**, forensics, and mitigation taking time from core mission delivery

Reputation and Privacy

- **Negative** impact on the State/Agency's **reputation** to secure tax and revenue as well as other personal identifiable information entrusted by citizens and businesses

So you've been breached…

…there are specific steps to consider taking

- ✓ Isolate the environment, but don't shut it off
- ✓ Find someone with the right skillset to assist
- ✓ Maintain the chain of custody
- ✓ Identify and isolate the reason for the breach
- ✓ Understand your exposure
- ✓ Determine your stakeholder audience
- ✓ Empathize, sympathize,
  but be cautious about apologizing

Preparing for the inevitable

“Security is not a discrete problem to be solved, but an ongoing challenge to be managed” – Tech Trends 2013 – A public sector perspective , Deloitte

Four lessons from the front lines

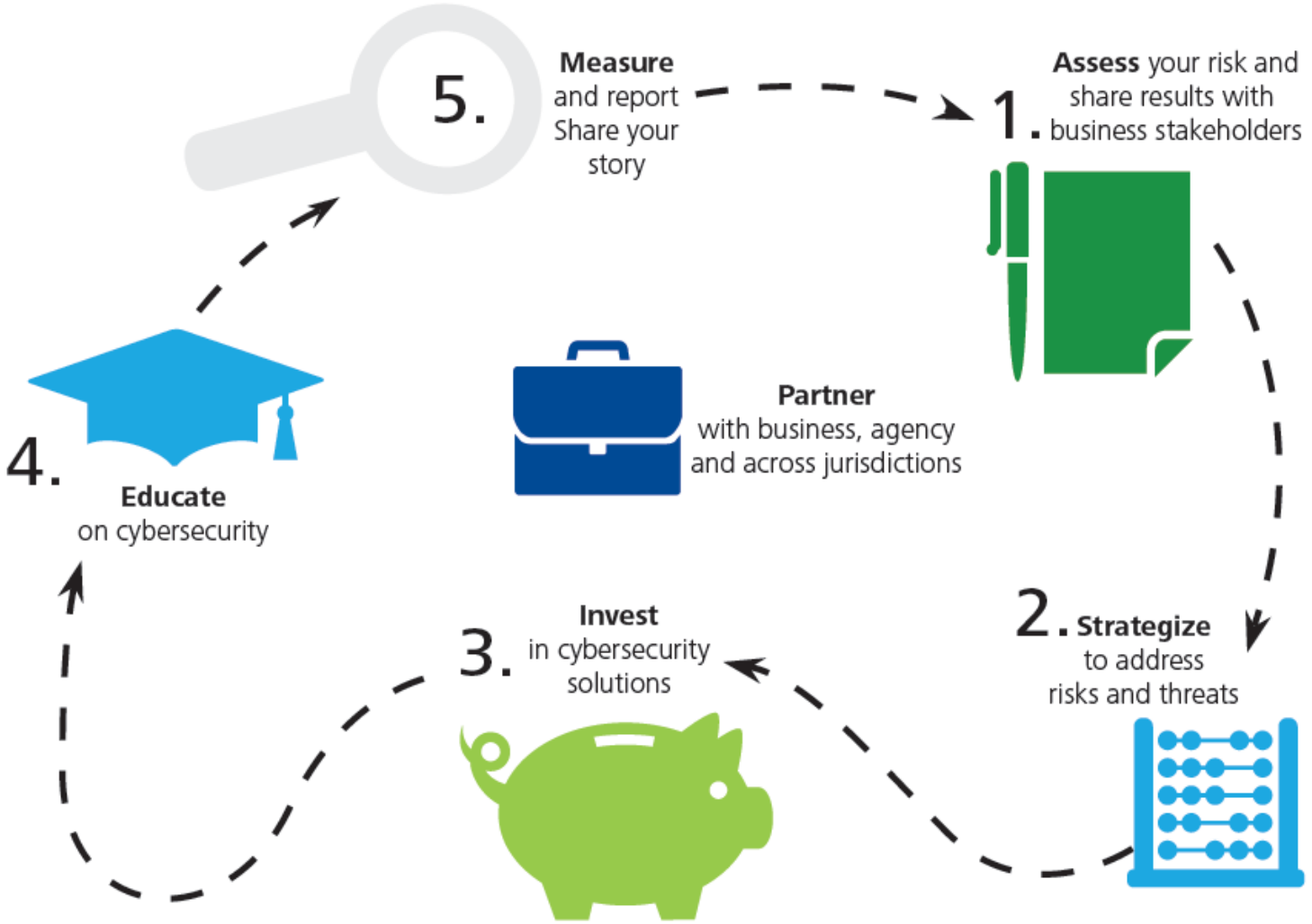
Considerations for the public sector…

1. **Start with a risk driven approach**
2. **Do not let cost pressures steer you off-track**
3. **Improving security can enhance ease of use**
4. **Use procurements and acquisitions to find better security approaches**

Source: Deloitte Tech Trends 2012: A public sector perspective

Achieving a persistent state of cyber-readiness

Establishing a culture of collaboration and awareness



Source: Deloitte Tech Trends 2012: A public sector perspective

Tactics to improve States' cyber-preparedness

Actions to move your program forward…

- ✓ Assess and communicate security risks
- ✓ Better articulate risks and audit findings with business stakeholders
- ✓ Explore creative paths to improve cybersecurity effectiveness within states' current federated governance models
- ✓ Focus on audit and continuous monitoring of third-party compliance
- ✓ Raise stakeholder awareness to combat accidental data breaches
- ✓ Aggressively explore alternative funding sources including collaboration with other entities
- ✓ Make better security an enabler of the use of emerging technologies

Source: 2012 Deloitte-NASCIO Cybersecurity Study

Homework

Ask yourself the following questions…

- Do we really understand our potential exposure?
- Are we appropriately protecting our sensitive information?
- When was the last time we checked?
- Do we have the right response plan?
- Are we ready to answer to the public?

Questions?

Deloitte.

Daniel Gabriel
Senior Manager
Security & Privacy
State and Local Government

Deloitte & Touche LLP
550 S Tryon St
Charlotte, NC 28202
USA

Tel: + 1 704 887 1654
Mobile: + 1 704 615 1777
dgabriel@deloitte.com

Member of
Deloitte Touche Tohmatsu Limited

Deloitte.

Srini Subramanian
Principal
Security & Privacy
State and Local Government Lead

Deloitte & Touche LLP
300 Corporate Center Drive
Camp Hill, PA 17011
USA

Tel: + 1 717 651 6277
Mobile: + 1 717 805 0364
ssubramanian@deloitte.com

Member of
Deloitte Touche Tohmatsu Limited

End notes

1 Ellen Messmer , Gartner reveals Top 10 IT Security Myths, Network World, June 11, 2013, http://www.networkworld.com/news/2013/061113-gartner-reveals-top-10-it-270738.html?page=2

2 Data Loss Statistics, Open Security Foundation, July, 2013, http://datalossdb.org/statistics

3 Tech Trends 2013: A public sector perspective, Deloitte, www.deloitte.com/us/publicsectortechtrends, pages 102 – 106.

4 2012 Deloitte-NASCIO Cybersecurity Study:, State Governments at Risk: A call for collaboration and compliance, Deloitte and the National Association of State Chief Information Officers, October, 2012, www.deloitte.com/view/en_US/us/Services/audit-enterprise-risk-services/Security-Privacy-Services/23eac2887a97a310VgnVCM2000003356f70aRCRD.Htm.

5 Mike Lennon, Texas Comptroller's Office Left Unencrypted Data of 3.5 Million on Publicly Accessible Server, Securityweek, April 11, 2011, http://www.securityweek.com/texas-comptroller%E2%80%99s-office-left-unencrypted-data-35-million-publicly-accessible-server

6 Ben Worthen, What to Do if You've Been Hacked, The Wall Street Journal, September 26, 2011, http://online.wsj.com/article/SB10001424053111904265504576566991567148576.html

7 Prescott E. Small, Defense in Depth: An Impractical Strategy for a Cyber World, The SANS Institute, November 14, 2011, http://www.sans.org/reading_room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world_33896

End notes (cont.)

8 Mark Mazzetti and Michael S. Schmidt, Ex-Worker at C.I.A. Says He Leaked Data on Surveillance, The New York Times, June 9, 2013, http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?pagewanted=all&_r=0

9 Charlie Savage, Edward Wyatt, Peter Baker, and Michael D. Shear, Intelligence Chief Calls Leaks on U.S. Data Collection 'Reprehensible', The New York Times, June 7, 2013, http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?pagewanted=all&_r=0

10 David Alexander, U.S. defense chief says Snowden leaks were 'serious security breach', Reuters, June 26, 2013, http://www.reuters.com/article/2013/06/26/usa-security-hagel-idUSL2N0F21HB20130626

11 Ponemon Institute LLC , 2011 Cost of Data Breach Study: United States, March 2012, http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Member of Deloitte Touche Tohmatsu Limited