



CTI is IT

**business technology without
limits**

Collin Freebourne Jr.
Professional Services Manager – CISSP, CCSP, CISA,
STS-CCS

Agenda – Current Security Threats

- **CTI Overview**
- **What's the problem?**
- **Who is the “Threat Agent”?**
- **How should you respond?**
- **Other areas of concern**
- **Q&A**

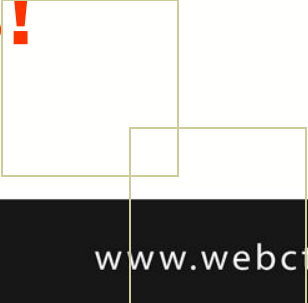


A little bit about CTI...



- Formed In 1985
- Geographic Footprint –Maryland, DC, Southern Pennsylvania,
- Finance, Education, Healthcare
- Highly Certified, Tenured Engineers

**We Design, Integrate,
and Support Solutions!**

A decorative graphic consisting of three overlapping squares with thin black outlines, positioned to the right of the main text.

www.webcti.com



CTI's Core Competencies

Security

Compliance

**Disaster Recovery &
Business Continuity**



Core Solutions

The SOLUTIONS that map to our
CORE COMPETENCIES include...

Data Archiving

**Platform
Upgrades**

**Enterprise
Storage**



**Infrastructure
Security**

Virtualization

**DR Design/Colo
Services**



CTI Vendor Partners

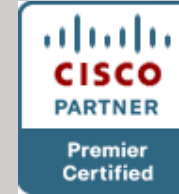
We hold close partnerships with
Strategic Manufacturers



Symantec Gold Partner



Gold Partner



Gold
Solution Advisor



Some of our customers



Some of our customers



Why so many data breaches?



What's the problem?

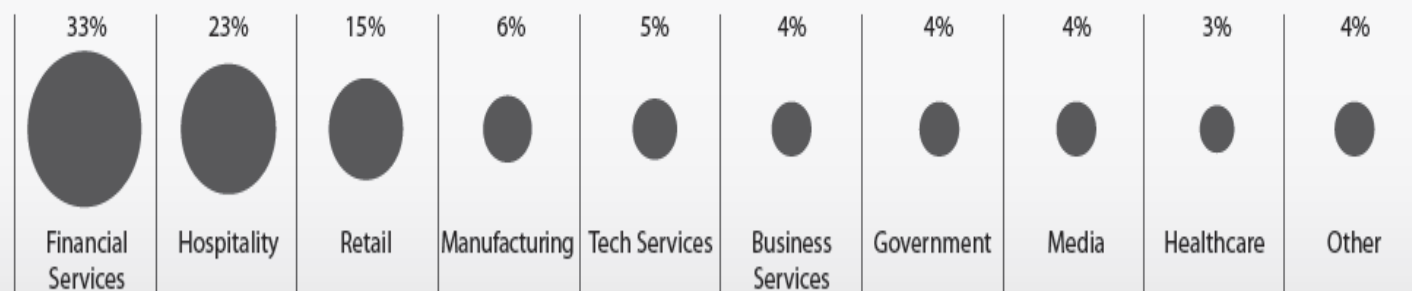
- More people are performing financial transactions online.
- Many organizations and consumers are not implementing the level of information security necessary to protect data. Should they have to? How much is enough?
- The anonymity of the Internet offers a veil as well as new opportunities/victims.
- Tough global economy.
- The “Love of money”. Where is the money?



Data Breaches by Industry



Figure 1. Industry groups represented by percent of breaches



Recent Publicized Data Breaches

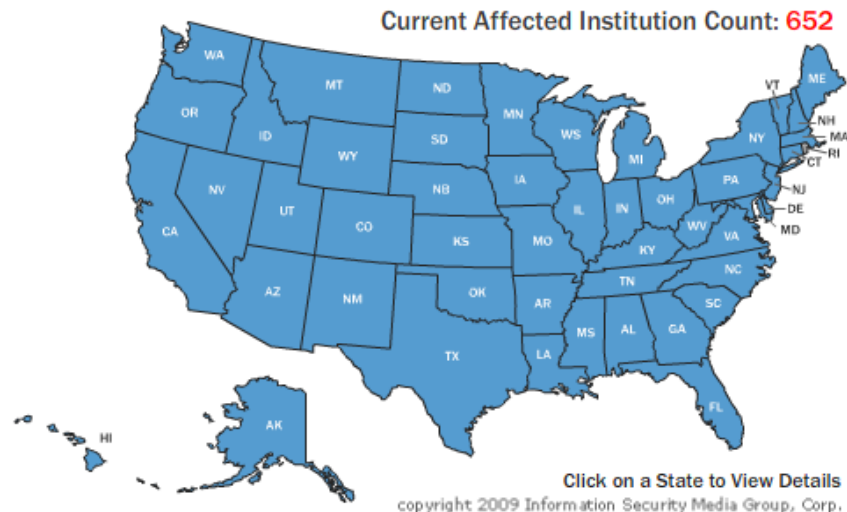


- **6 of the top 10 largest data breaches of the decade involved financial companies.**
 1. **Heartland Payment Systems – 2009:** In what has been called the largest credit card crime of all time.
 2. **TJX Companies – 2007:** credit card.
 3. **U.S. Department of Veterans Affairs – 2009:** The personal information for as many as 76 million veterans.
 4. **Card Systems -- 2005:** credit card.
 5. **Veterans Laptop With Personal Data Stolen – 2006:** Stolen laptop with personal information.
 6. **Bank of New York Mellon – 2008:** Personal information.
 7. **Certegy – 2007:** Check Services.
 8. **TD Ameritrade – 2007:** Customer information.
 9. **CheckFree – 2008:** Redirected customers to a Web site hosted in Ukraine that tried to install malware on peoples' computers.
 10. **Hannaford Bros. Chain – 2009:** Stolen credit and debit card numbers.

Heartland Payment System's Breach

Update: Thousands of Institutions Impacted

See the interactive map below for a comprehensive list (updated daily) of institutions affected by the breach. This list represents only those institutions that have *reported* their connection to the breach. Experts estimate the total number of affected institutions in the thousands.



The list of affected institutions is drawn from: Information provided to us by institutions; news reports from local and national media outlets; and announcements posted on institutions' websites.

Heartland Payment System's Breach - MD

Click Anywhere to Return to Map

Maryland
Provident Bank, Baltimore, MD
Bay Vanguard FSB, Baltimore, MD
Beverly National Bank, MD
Cedar Point Federal Credit Union, Lexington Park, MD
Madison Square Federal Savings Bank, Baltimore, MD
Maryland Bank and Trust Co., Lexington Park, MD
NIH Federal Credit Union, Rockville, MD
Rosedale Federal Savings & Loan Association, Baltimore, MD
St Agnes Employees FCU, Baltimore, MD (550)

Click on a State to View Details

Copyright © 2009 Information Security Media Group, Corp.

The image shows a map of Maryland with several lines pointing to specific locations. The map is overlaid with a list of financial institutions and their locations. The list includes: Provident Bank, Baltimore, MD; Bay Vanguard FSB, Baltimore, MD; Beverly National Bank, MD; Cedar Point Federal Credit Union, Lexington Park, MD; Madison Square Federal Savings Bank, Baltimore, MD; Maryland Bank and Trust Co., Lexington Park, MD; NIH Federal Credit Union, Rockville, MD; Rosedale Federal Savings & Loan Association, Baltimore, MD; and St Agnes Employees FCU, Baltimore, MD (550). The map also shows parts of Pennsylvania (PA), West Virginia (WV), and Virginia (VA). The text 'Click Anywhere to Return to Map' is at the top right, and 'Click on a State to View Details' is at the bottom right. A copyright notice for Information Security Media Group, Corp. is at the bottom center.



Not in Maryland! I am too small!

M&T Bank
Baltimore, MD
Records Taken: 39
Type of Breach: Missing Paper Documents
Date: March 1

M&T Bank reported to the Maryland Attorney General in a letter dated December 18, 2009 that a courier carrying work for a Baltimore branch was robbed on December 15, 2009. In the courier's bag were 39 customers' checks.

Partnership Federal Credit Union
Washington, DC
Records Taken: 22
Type of Breach: Accidental breach
Date: March 1

The Partnership Federal Credit Union reported to the Maryland Attorney General on July 22, 2009 that an internal data file had been discovered on a computer outside of the secured network earlier in the summer. This may have potentially exposing personal and financial information. The letter was posted to the OAG website on March 1.

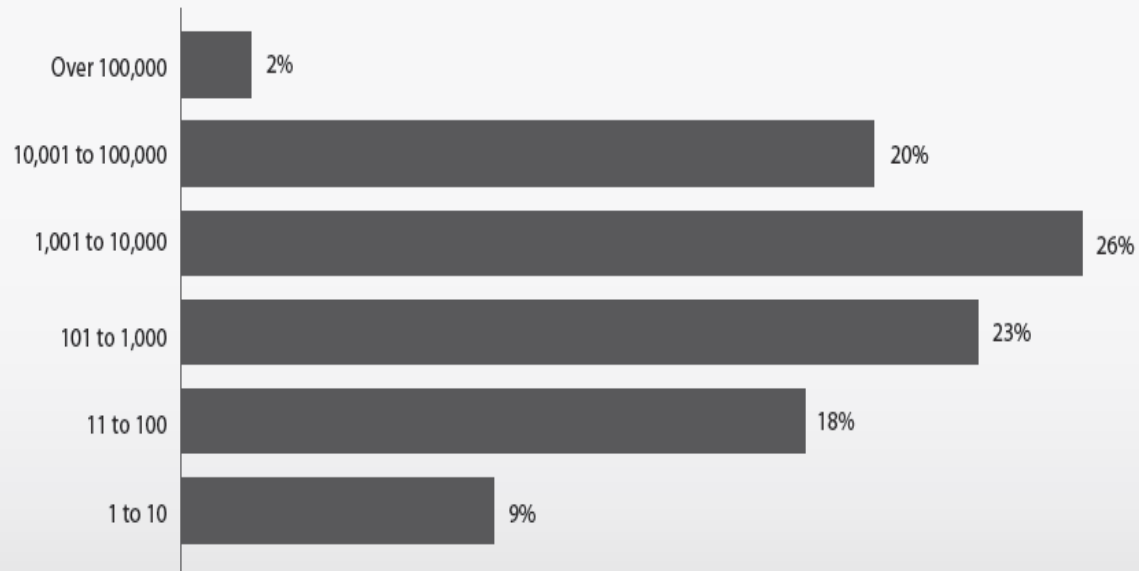
Telhio Credit Union
Columbus, OH
Records Taken: Unknown
Type of Breach: Insider Theft
Date: March 1

Telhio Credit Union reported to the Maryland Attorney General in a December 22, 2009 letter that a former employee had downloaded a report with customer personal and financial information before leaving his employment in early August 2009. One Maryland resident's information was in that report. It was not stated how many others may have been affected nationwide.



I am too small, Really!

Figure 4. Organizational size by percent of breaches (number of employees)



Cost of Data Braches



Who is the “Threat Agent”?

WHO IS BEHIND DATA BREACHES?

70% resulted from external agents (-9%)

48% were caused by insiders (+26%)

11% implicated business partners (-23%)

27% involved multiple parties (-12%)

HOW DO BREACHES OCCUR?

48% involved privilege misuse (+26%)

40% resulted from hacking (-24%)

38% utilized malware (<>)

28% employed social tactics (+16%)

15% comprised physical attacks (+6%)



Who is the “Threat Agent”?

“Only 15% of employers perform an audit of the documents that former employees leave with.”¹¹

“59% of laid-off and departing employees admit taking data with them—of those, 79% say their former employer had a policy against the practice.”¹²



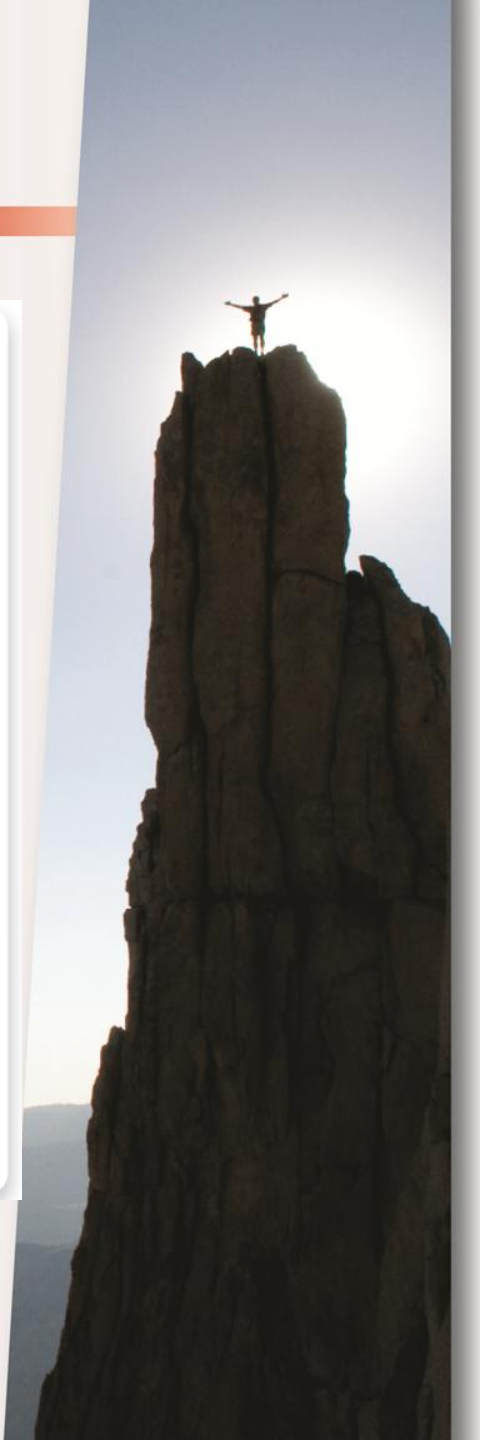
Who is the “Threat Agent”?

Finance IT Workers Rank the Industry’s Riskiest Insiders

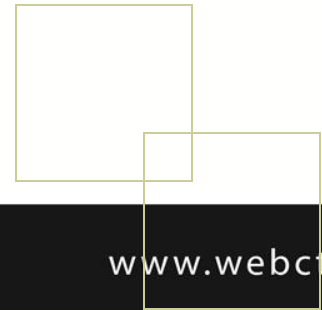
- » **Tellers and Traders:** ranked high-risk by 60% of respondents
- » **Administrative/Back Office Workers:** ranked high-risk by 55.74% of respondents
- » **Technology Workers:** ranked high-risk by 34.43% of respondents
- » **Executive/Senior Management:** ranked high-risk by 29.51% of respondents
- » **Call Center Employees:** ranked high-risk by 29.51% of respondents
- » **Line of Business Employees:** ranked high-risk by 26.63% of respondents¹³

Table 2. Types of internal agents by percent of breaches within Internal

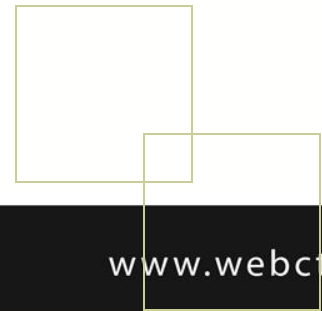
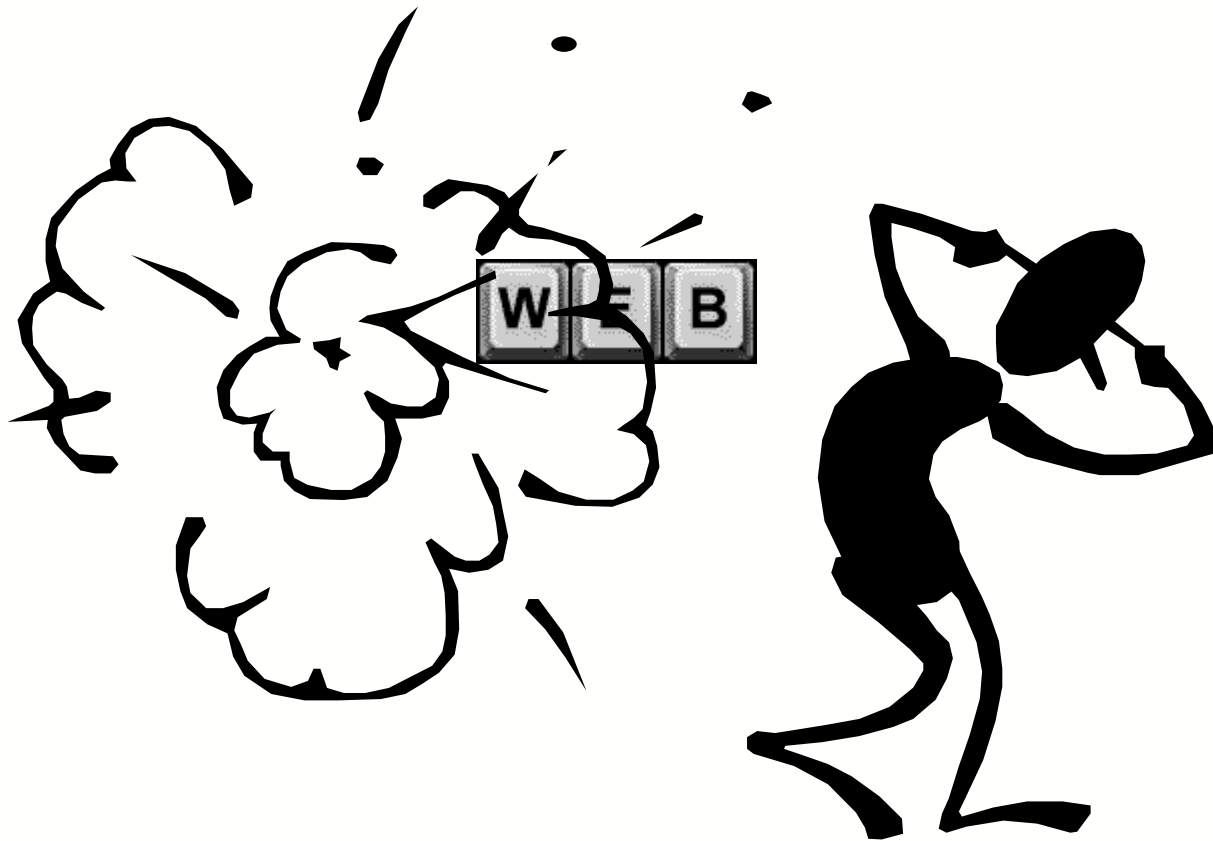
Regular employee/end-user	51%
Finance/accounting staff	12%
System/network administrator	12%
Executive/upper management	7%
Helpdesk staff	4%
Software developer	3%
Auditor	1%
Unknown	9%



How should you respond?



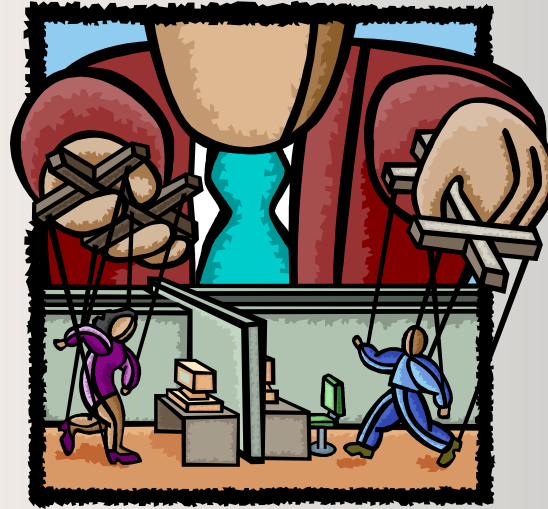
How should you respond?



www.webcti.com



How should you respond?



**Get Executive Management
Involved!!!!**

How should you respond?

- Discover & Assess Risk
 - ✓ Eliminate unnecessary data; keep tabs on what's left
 - ✓ **Find a competent IT partner and build strategic alliances. (Wink Wink – CTI)**
 - ✓ Work with other larger, smaller or similar size organizations and pick their brains.

- Establish & Enforce Policy
 - ✓ Ensure essential controls are met
 - ✓ Check the above again
 - ✓ Fix Open Vulnerabilities
 - ✓ Test and review web applications



How should you respond?

- Filter outbound traffic
- Audit
 - ✓ Audit user accounts and monitor privileged activity
- Monitor and mine event logs
- Don't forget about mobile devices!!!

Other areas of concern

- Mobile Banking
- Bluetooth Security



Questions?



Thank You!

business technology without limits

