Cybersecurity: It's not just for businesses

BAKER TILLY

Candor. Insight. Results.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP,
an independently owned and managed member of Baker Tilly International.

Introduction

BAKER TILLY

Candor. Insight. Results.

- For many entities, business value resides in its **data and network** systems
- A sophisticated community of "hacktivists," organized cyber criminals / syndicates, and state-sponsored spies, wants to cause **competitive harm** by exploiting technical and social vulnerabilities of information assets
- This combination leads to a **high-likelihood of data breaches**

BAKER TILLY

Candor. Insight. Results.

They mess up your stuff just because:

- …they don't like you
- …they don't like your mission
- …they can

BAKER TILLY

Candor. Insight. Results.

Cyber criminals are organized and operate like a business, focused on the profit motive:

- Identity theft
- Fraudulent credit card transactions
- Ransomware

State-sponsored cyber espionage

BAKER TILLY

Candor. Insight. Results.

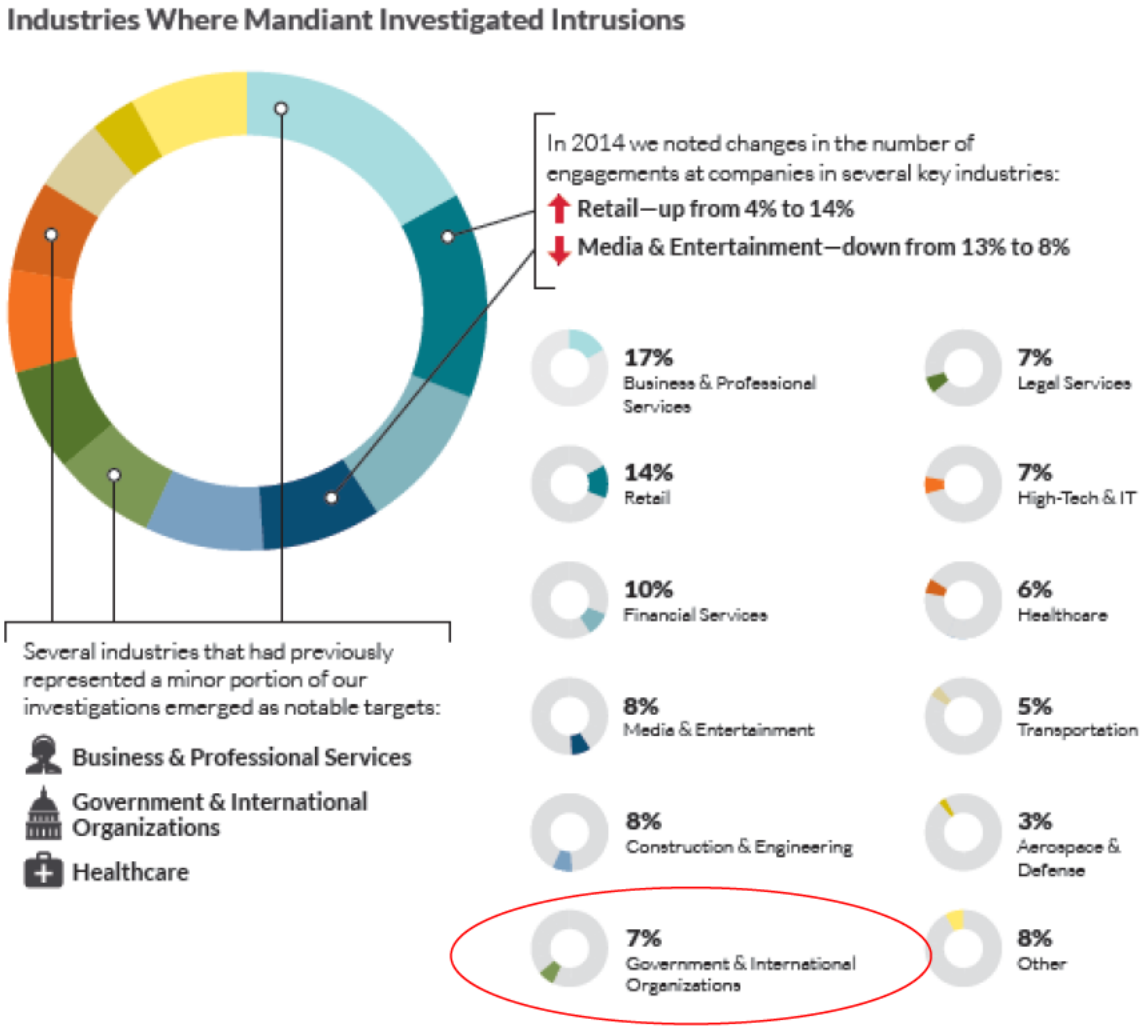
We have enemies who don't like our national policies and want to destabilize our economy. This is known as cyberterrorism or cyberwarfare.

View the Mandiant report at:
intelreport.mandiant.com

Industries targeted by cyber threats

BAKER TILLY

Candor. Insight. Results.



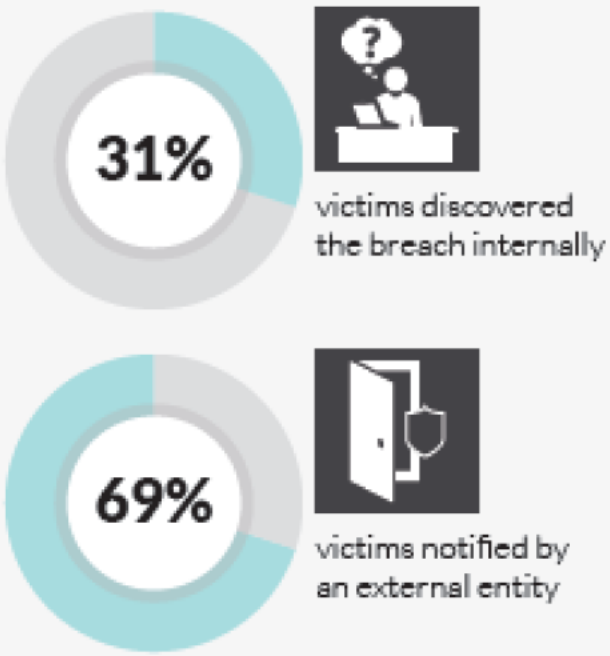
Source: Mandiant M-trends 2015 Threat report

How compromises are detected

BAKER TILLY

Candor. Insight. Results.

How Compromises Are Being Detected



Time from Earliest Evidence of Compromise to Discovery of Compromise

median number of days that threat groups were present on a victim's network before detection

24 days less than 2013

Longest Presence: 2,982 days

Source: Mandiant M-trends 2015 Threat report

Evolving cyber-risk landscape

BAKER TILLY

Candor. Insight. Results.

Past	Present	Impact on Risk
Mostly physical assets (plants, equipment) - relatively few digitized assets.	Highly digitized asset base (IP, financial, PII), mobile and cloud technologies.	> More data and platforms to secure and manage > Data can be outside of your control > More people with access to data
Simple, unsophisticated attacks (e.g., web site defacement intended to embarrass).	Advanced Persistent Threats (APTs) involve high degree of complexity and sophistication.	> Bad actors are dedicated professionals > Need to defend against professional grade tools
Relatively self-contained IT environment with limited use of 3rd parties for hosting and cloud services.	Concept of "digital ecosystem" involving outside stakeholders and 3rd parties/vendors.	> Potential for undefined /unverified security obligations and vendor responsibilities
IT budgeted HW/SW expenditures; managed deployment and use.	Departments outside of IT can implement rogue cloud services.	> Lack of control over enterprise data
Limited use of mobile data access. IT provided a restricted list of mobile device choices which provided robust security support.	Mobile user access to applications containing personal/financial data and use of BYOD is nearly commonplace.	> More challenging for IT to assure security of "end point" devices.

What does it mean for governmental entities?

BAKER TILLY

Candor. Insight. Results.

- Entities should expect to get hacked and to be breached
- Robust cyber security management programs are needed to manage the risk to the entity
- Stakeholders in the cyber security management program are cross-functional—not just IT

Key components of effective cybersecurity programs

BAKER TILLY

Candor. Insight. Results.

01 - Data classification and security risk assessment

BAKER TILLY

Candor. Insight. Results.

- Understand all information systems at a granular level
- Figure out what assets really matter (crown jewels)
- Translate and align to entity objectives and priorities
- A clear definition of risk tolerance levels is required
- The assessment must be unique to the entity and its industry
- The process must be iterative and dynamic, adopting to constant change
- Standard frameworks improve effectiveness (e.g., NIST, COSO)

02 - Security control implementation

BAKER TILLY

Candor. Insight. Results.

- Policies and procedures must be documented
- Layered security is critical (multiple lines of defense)
- Use a combination of preventative and detective controls (IT and business controls)
- Support with cyber-focused standards (e.g., ISO, SANS, NIST)
- Event correlation is becoming increasingly important
- Ongoing assessment is critical to keep pace with change
- Ultimately, controls must be deployed that are commensurate with the value of the assets you are trying to protect
- Don’t forget security awareness training for users

03 - Security control verification

BAKER TILLY

Candor. Insight. Results.

- Validate that security controls are properly designed and implemented
- Test effectiveness through internal and external vulnerability and penetration testing
- Leverage independent experts (similar to traditional internal audit function) to validate controls
- Establish security baseline metrics and measure efficacy over time
- Identify improvement opportunities
- Promote changes to enhance the overall security posture

04 - Breach response planning and testing

BAKER TILLY

Candor. Insight. Results.

- Anticipate “when” not “if”
- Identify threats and plan realistic scenarios to test systems
- Document formal response and recovery procedures
- Practice in an environment that allows consideration without urgency
- Based on test results, identify gaps and areas for improvement
- Distribute plan, procedures, and testing results to stakeholders to raise awareness
- Practice makes perfect*

05 - Risk acceptance and transfer

BAKER TILLY

Candor. Insight. Results.

- Comprehensive risk consideration
- Acceptance: cost to mitigate > risk reduction
- Transfer: let someone else pick up the tab
- Understand cyber-liability policies and the ability to limit financial impact of a security breach
- Evaluate agreements with third parties to understand contractual responsibilities related to risk
- Regularly re-evaluate systems during risk assessments

Summary

BAKER TILLY

Candor. Insight. Results.

- Effective cybersecurity management doesn't mean you won't get hacked
- Effective cybersecurity management programs need to start with solid data classification and a security-focused risk assessment
- Effective cybersecurity management is a continuous process

Disclosures

BAKER TILLY

Candor. Insight. Results.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2015 Baker Tilly Virchow Krause, LLP.