# Watkins Consulting

# &

# Watkins | Meegan

# Cyber Security and Risk Management

**How effective is your financial institution's cyber security and risk management strategy?**

The greatest risks posed to today's financial institutions are often those not considered until a security incident or breach occurs. The penalties for security breaches are severe. Identification and evaluation of potential risks has become even more challenging with the advent of cloud computing, social media strategies and our over reliance on technology tools.

# Introductions

Richard Kozlow
Senior Director, Watkins Consulting
rkozlow@watkinsconsulting.com

Gregory A. Brake
Director, Applied Discovery
greg.brake@applieddiscovery.com

Jim Jaeger
VP of Cybersecurity Services, General Dynamics
jim.jaeger@fidelissecurity.com

Bhavesh Vadhani
Director, Watkins Meegan
Bhavesh.vadhani@watkinsmeegan.com

# Cyber Security
# ...a game of numbers

Richard P. Kozlow, Senior Director
Watkins Consulting, Inc.

# Assumptions...

- Defensive systems are state-of-the-art

- They detect & defeat every intrusion as it happens...or soon thereafter

# 17%

**...the percent of on line Intellectual Property thefts that go UNDETECTED for <u>one month</u> or more**

# 31%

...the percent of on line Intellectual Property thefts that go **undetected** for ONE YEAR or more

- "How Safe is your data?" – WSJ/Michael Chertoff 1/18/13

# UNIT 61398

...”A Shanghai-based

**Chinese military team**

that since 2006 has mounted cyber assaults to steal terabytes of codes and other information from US assets.” – Mandiant (a private security firm)

# Advance Warnings

- ..."Cause the enemy nation to fall into social panic, street riots, and a political crisis." – 1999

- "Direct Information Warfare" – 2002

# Galaxy of Players

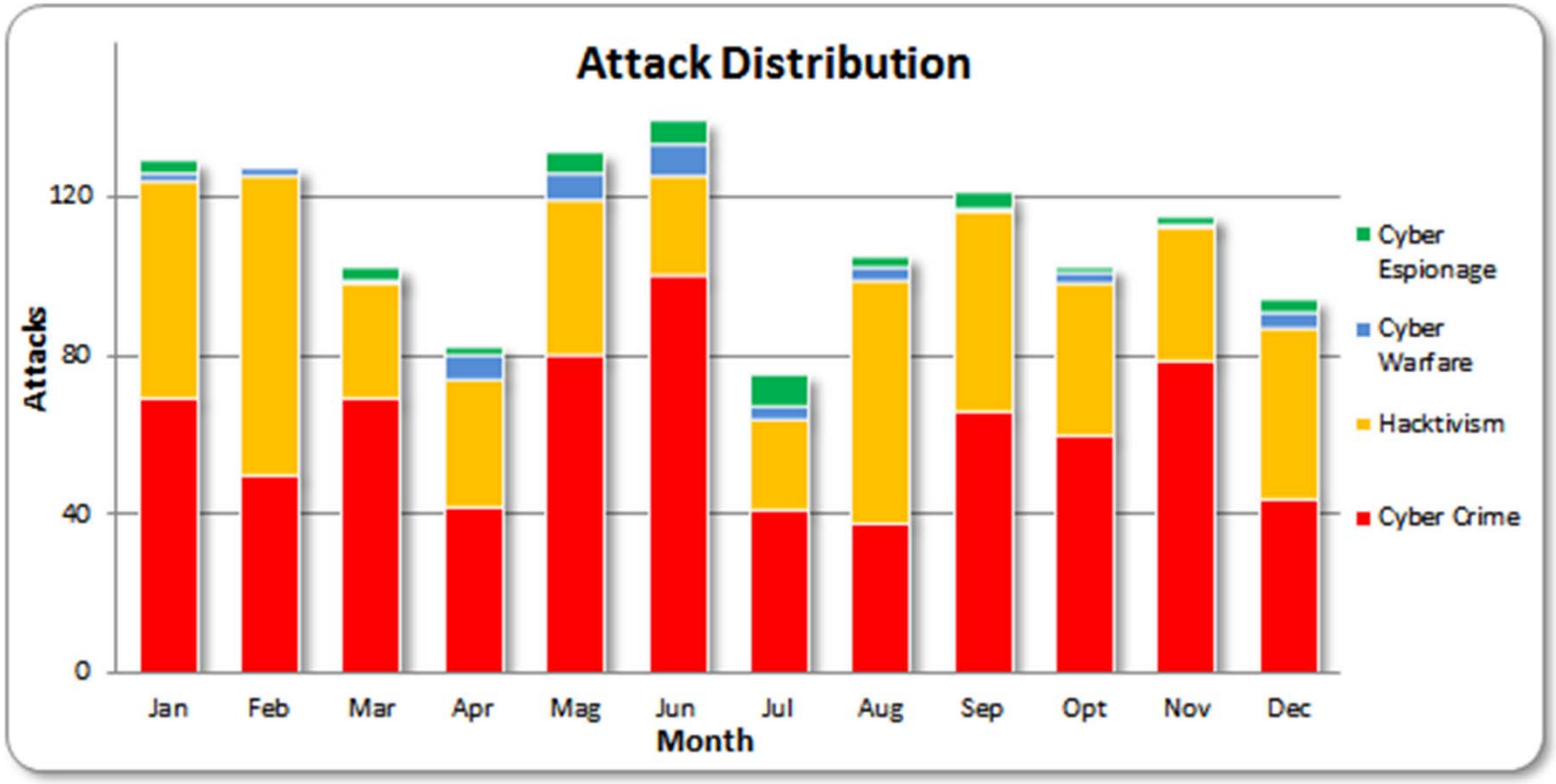
- State-sponsored
  - China
  - Russia
  - Iran
  - Israel
  - U.S.
- Cyber Criminals – Run like a Business!!
  - Data thieves/exploitation
  - On line fraud
  - Intellectual property/ransom, sale, exploitation

# Galaxy of Players

- Insiders
  - Supply Chain
  - Employees/contractors
- Traditional hackers
- Hacktivists
  - Growing % of intrusions
  - Motivations not always clear

# 2012 Cyber Attacks

Source: hackmageddon.com



# BYOD

The explosion of smartphones and a desire to save money

Result:

- A proliferation of

  "bring your own device" policies

But...

# More numbers to consider...

84%

&

47%

**84%** of non-IT individuals surveyed in North America use the same smartphone for personal and work-related activities...

and

...**47%** of those individuals have **NO PASSWORD** on their mobile phone.

-*Internal Auditor*, October, 2012

# Who you gonna call?

Federal Legislation:

- Aimed at promoting sharing of information

  Bogged down since 2011

# Resources

- Risk Management Strategy
- Legal input
- Marketing & Operations rollout
- Have a Plan

# Process

Must EVOLVE interactively…

…the bad guys are evolving DAILY

# Network Defense & Forensics

# Cyber Services

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

## Cyber Threat to Financial Services Industry

**The new world currency is information**

- Intellectual Property
- PII, PHI, credit card and other banking data
- Merger & Acquisition

**China and Russia are the good actors**

- Rational
- Not likely to destroy US Financial Services Industry
- *traditionally…*
  - China – IP
  - Russia – Banking
- Organized criminals – US, UK, Japan and other innovative nations

# Cyber Threat to Financial Services Industry

## China continued

- Large Private Equity Firm recently discovered China has been inside their network for 6-8 months
- Must Grow 7%
- Last year GDP 9 times what it was in 1990
- This year 7.7%
- Where is their future growth going to come from?
    - *Research and development?*

## Cyber Threat to Financial Services Industry

**North Korea & Iran:**

- "Destroy economic prosperity of the US"
- Kim Jong-un
  - Attacked South Korea FSI
- Iran
  - Attacked Aramco
    - All financial transactions re oil and gas
    - Destroyed 30,000 computers/servers
  - Probing US Financial Services Industry now
  - Moving beyond big 5 banks
    - Industry infrastructure

## Emerging Trends

**Employ integrated Legal - Cyber Services Team to manage breach incident response:**

- Law firms - weak link in corporate cyber security strategy
  - Vendor security audits
- Standing Master Services Agreements enable rapid response
- Privilege protection to investigative data
  - CISO reporting to General Counsel
  - Heightened litigation risk
- Proactive Breach Response Plan
  - Assessment
  - Team identification

## Emerging Trends

- **Ecosystem to handle all phases of breach response**
  - Forensic investigation
  - Containment and remediation
  - Law enforcement engagement
  - Regulatory dialog
  - Litigation support
  - Cyber Insurance claims
  - Reputational Risk – PR

# 2012 Attack Vectors

30%: SQL Injection

15%: Advanced Attacks

15%: Insider

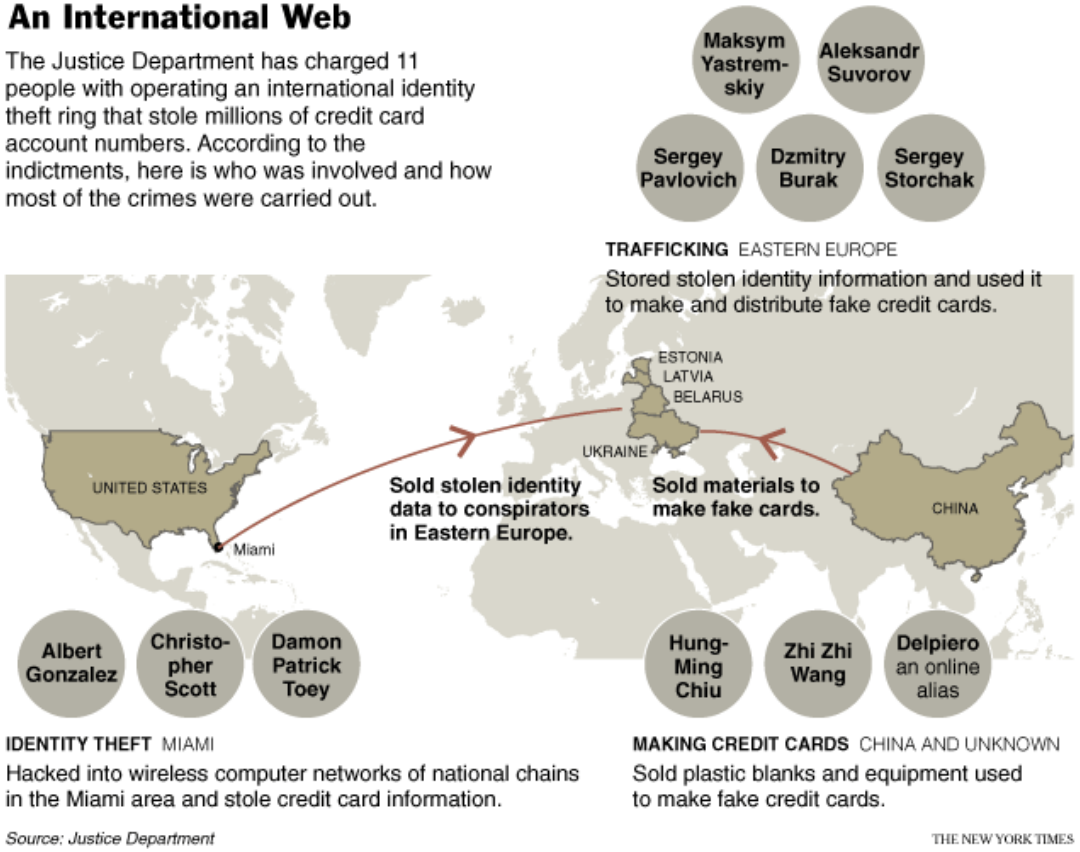
25%: Phishing

5%: Wireless

Source: Compilation of Breaches Investigated, GDAIS 2012

# The Concern is Driven by Both Cost and Reputational Impact

- TJX reported 46 million credit/debit card numbers stolen
- U.S. Justice Department got arrests and convictions against the criminals
- But TJX spent $132 million on expenses related to the breaches



## Example Investigations – Debit Card ATM Thefts

### Breaches followed by ATM cash outs

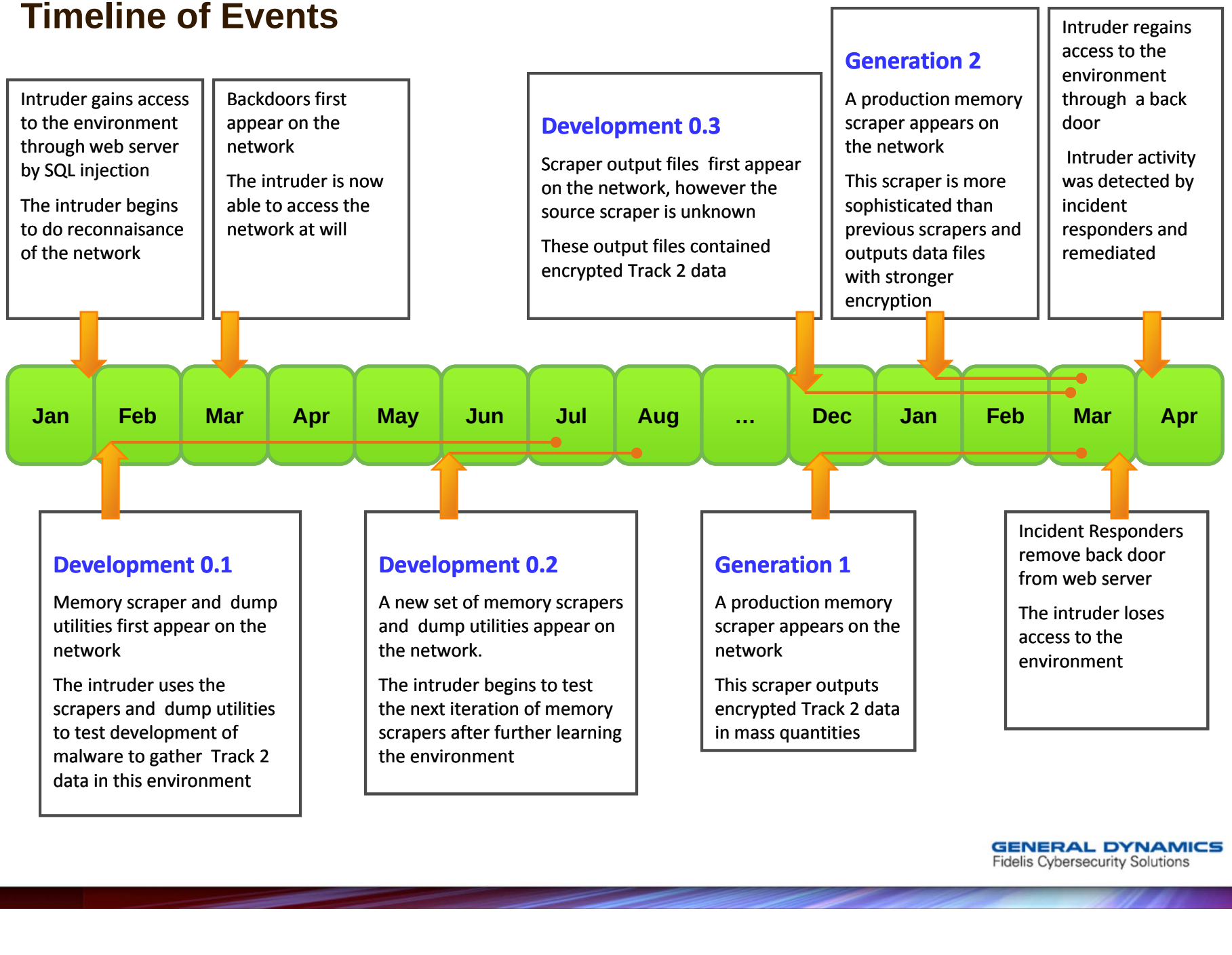
- About $10M ATM from in 24 hours
- 200 - 300 cities worldwide
- “Cashers” use about counterfeit cards and PINs
- Raised limits, multiple same-day withdrawals

**First exploitation of HSMs to derive PINs**

**First arrests and convictions in Russia for cyber crime in US**


***Director, FBI Cyber Division cited information sharing and partnership between cyber forensics firms and law enforcement as the key to achieving arrests and convictions***

# Timeline of Events



# The Incident Response Team – Key Stakeholders

- Client
  - Executives
  - Technology Owners
  - Business Operations
- Counsel
  - Internal
  - External
- Law Enforcement
  - DOJ, USAGO
  - USSS, FBI
- Third-Parties
  - Regulators (FTC, SEC, FFIEC, Fed Reserve, OCC)
  - Auditors
  - Credit Card Brands
  - Vendors

# FBI Director Mueller

- *"There are only two types of organizations: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again," Mueller said.*

- *"State-sponsored hackers are patient and calculating," Mueller said. "They have the time, money and resources to burrow in and wait. You may discover one breach only to find that the real damage has been done at a much higher level."*

Source: CNNMoney http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm?iid=EL; last accessed 10.24.12





12

## Proactive Defense Services

- **Establish a state of readiness**, improve your overall security posture, reduce the likelihood of a compromise, prepare yourself to respond effectively…
  - Security architecture and engineering
  - Security policy development
  - Security strategy workshops
  - Threat identification and vulnerability assessment
  - **Breach Indicator (BI) Assessments**
  - Penetration testing and network hardening
  - Compliance assessment and verification
  - Incident response planning and training

## Our Mission

Applied Discovery and General Dynamics Fidelis Cybersecurity Solutions provide organizations the power to face **advanced threats** with confidence with a robust, comprehensive portfolio of **products**, **services** and **expertise**.

*"If your organization is at a high risk for an APT attack, act as if you have already been compromised."*

*- Ernst & Young, Countering Cyber Attacks, April 2010*

# CYBER SERVICES CONTACTS:

Greg Brake, Applied Discovery

Ph: 202-480-0442

greg.brake@applieddiscovery.com

Jim Jaeger, GDFidelis Cybersecurity Solutions

Ph: 443-926-1159

jim.jaeger@fidelissecurity.com

# CYBER SECURITY…ADDITIONAL POINTS TO CONSIDER

# Cost of data breach these days?

- The average organizational cost of a data security breach in the U.S. in 2011 - $5.5 Million
- The average cost per record in the US in 2011 - $194
- The average cost per record in the US in 2011 for financial industry - $247

*- 2011 Cost of Data Breach Study: United States by Ponemon Institute*

# 2013 Threat Predictions

- Mobile worms on victims' machines that buy malicious apps and steal via tap-and-pay NFC
- Malware that blocks security updates to mobile phones
- Mobile phone ransomware "kits" that allow criminals without programming skills to extort payments
- Covert and persistent attacks deep within and beneath Windows
- Rapid development of ways to attack Windows 8 and HTML5
- Large-scale attacks like Stuxnet that attempt to destroy infrastructure, rather than make money
- A further narrowing of Zeus-like targeted attacks using the Citadel Trojan, making it very difficult for security products to counter
- Malware that renews a connection even after a botnet has been taken down, allowing infections to grow again

# 2013 Threat Predictions

- The “snowshoe” spamming of legitimate products from many IP addresses, spreading out the sources and keeping the unwelcome messages flowing
- SMS spam from infected phones.
- “Hacking as a Service”: Anonymous sellers and buyers in underground forums exchange malware kits and development services for money
- The decline of online hacktivists Anonymous, to be replaced by more politically committed or extremist groups
- Nation states and armies will be more frequent sources and victims of cyberthreats

*- McAfee Labs*

# Contact us

Richard Kozlow
Senior Director, Watkins Consulting
rkozlow@watkinsconsulting.com

Gregory A. Brake
Director, Applied Discovery
greg.brake@applieddiscovery.com

Jim Jaeger
VP of Cybersecurity Services, General Dynamics
jim.jaeger@fidelissecurity.com

Bhavesh Vadhani
Director, Watkins Meegan
Bhavesh.vadhani@watkinsmeegan.com

# Watkins Consulting Inc.
## www.watkinsconsulting.com

# Watkins | Meegan
## www.watkinsmeegan.com