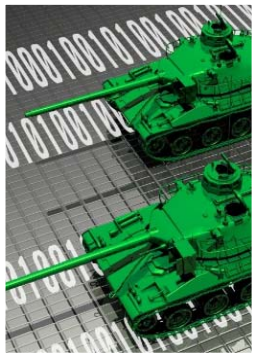
# Cyber Threats and Trends for Design Firms in 2019

**Jennifer Coughlin**, Partner, Mullen Coughlin, LLC

**Devon Ackerman**, Managing Director, Kroll

# Threats



**Nation State Actors (APT)**

**Organized Crime Groups**

Espionage

# Threats

## Ukraine

**2014**

**Attack -** VoIP DDoS

**Reason -** To facilitate the Russian annexation of Crimea

**Impact -** Government officials lost communications

**2016**

**Attack -** Power Grid

**Reason -** Ultimately unknown, although Russian Security Services were accused by the Ukrainian government of being responsible

**Impact -** 225,000 lost power, fear/intimidation?

# Threats

## Saudi Arabia

## 2017 (Shamoon)

**Attack -** Complete drive wiping

**Reason -** Iranian government accused by Saudi Government. Believe to be in response to Iran itself having suffering crippling Cyber attacks resulting in $67million in damages at a Petrochemical Complex.

**Impact -** 15 Saudi Government office and private companies shut down-system backups and core systems wiped.

# Threats

## NSA Derived SMB Exploit 2017 (WannaCry)

**Attack -** Ransomware spreading via SMB vulnerability

**Reason -** Financial gain through bitcoin payments for decryption key.

**Impact -** 100+ countries, potentially +200K hosts

- Hospitals w/x-ray equipment
- Nissan Vehicle manufacturing
- Fedex Package delivery infrastructure
- Russia Interior Ministry & Railroad systems
- Germany Railroad systems
- China University laboratories

# Threats

## Slingshot APT Group - 2018

**Attack -** Malware that infects routers and can stealthily collect network traffic data and information.

**Reason -** Unknown.

**Impact -**

- Middle East and African Nations
- Approximately 100 victim networks identified.
- As far back as 2012 with unknown initial infection vector.

# Threats

## The Trickle-Down Effect

- Cyber warfare between nations have focused on political, economic, and military advantages.
- Private networks are their battlegrounds.
- The nation state vs. nation state (Advanced Persistent Threat) attacks of years past are becoming the criminal attacks of present as cyber warriors and defenders…
  - perfect their craft
  - learn from their mistakes
  - learn from intrusions
  - document their successes and findings

# Trends - Business Email Compromises

- Phishing, Spoofing, Whaling,
  - AddressBook CarpetBombing
- “Please Remit Payment”
- “IT Password Reset”
- “Your Account is Locked”
- “Updated ACH Wire Instructions”

# Trends - Business Email Compromises

## Kroll Investigation

**Architectural Firm**

- Office 365, 1 account suspected of outbound spam
- Kroll investigated and identified 3 accounts
  - CEO, Secretary for CFO, and Comptroller
- Auto-forwarding rules -> external Gmail address (actor controlled)
- Earliest evidence of intrusion went back five (5) months
- 18,000 emails auto-forwarded

# Trends - Ransomware

- Coverage for intrusions
- Monetization goals
- Data destruction pre-Encryption

# Trends - Tech Support Fraud

- Fake customer or tech support
- Monetization goals
- Credential theft
- Intrusion vectors

# Trends - Third Party IT Services

- Common Remote Access Tool usage
- Common credential usage/re-usage
- Documented internal SOPs repeated across clients
- Client ticketing systems
- Audits for how your data is protected

# Trends - Third Party IT Services

- Audits for how your data is protected
- Restrictions on remote access
- Auditing on remote access
- Multifactor (2FA) for remote users

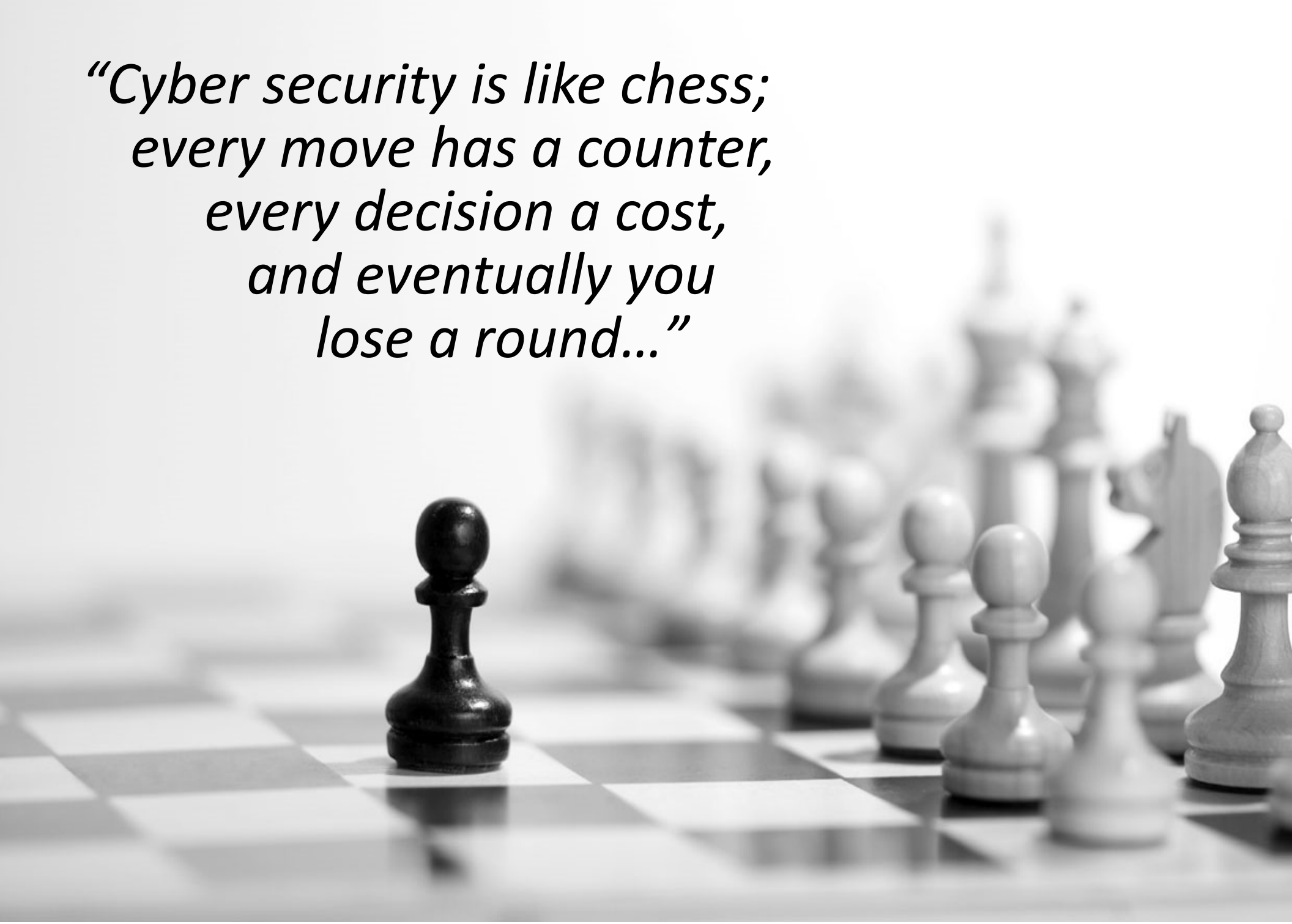
# Cyber Security - An Overview

**2011** **2018**

416 average day dwell time 78 average day dwell time

- **2017** - $676 million loss due to Business Email Compromises
- **2017** - $61 million due to Corporate Data Breach

- FBI - 2,982 days Kroll - 781 days


*“Cyber security is like chess;
every move has a counter,
every decision a cost,
and eventually you
lose a round…”*

# Resources

| | |
|---|---|
| About Digital Forensics & Incident Response (DFIR) | http://aboutdfir.com |
| Kroll Global Fraud and Risk Report | http://kroll.com |
| Multi-State Information Sharing and Analysis Center | http://cisecurity.org |
| U.S. Computer Emergency Response Team | http://us-cert.gov |
| Mandiant Intel Reports (APT1, APT28, FIN4) | http://intelreport.mandiant.com |
| Cylance “Operation Cleaver” Report | http://cylance.com |
| CSOonline Security and Risk News | http://csoonline.com |
| Internet Crime Complaint Center | http://ic3.gov |
| Wired.com Threat Level Blog | http://wired.com/threatlevel |
| NCIX Report | http://ncix.gov |
| Local InfraGard Chapters | https://infragard.org |
| Fatal System Error: The Hunt for the New Crime Lords | by Joseph Menn |
| Cyber War | by Richard Clarke |

*“For every security mechanism devised, there is someone who will defeat it.”*

Kroll | A Division of DUFF & PHELPS

devon.ackerman@kroll.com

linkedin.com/in/devonackerman

# Legal Considerations

- State law
- Federal Law
  - GLBA
  - SEC
  - DOE
  - FTC
  - HIPAA
  - FERPA
- International Law
  - GDPR
  - Canada
  - Australia
- Contract
  - PCI
  - Clients
  - Employees

- **Perform** risk assessments to understand the data within your organization and safeguards to protect the security of that data
- **Prepare and enforce** data security policies and procedures
- **Prepare and test** Incident Response Plan
- **Ensure** experience on the Incident Response Team
- **Document** your due care measures (training and enforcement) being taken
- **Insure** yourself with appropriate coverage at appropriate limits
- **Understand** contractual obligations
- **Execute** service level agreements
- Repeat

# Anatomy of a Breach Response

## BREACH DISCOVERY

EXPERTS
- Breach coach
- Forensics
- Public relations

INVESTIGATION - internal/forensic/criminal
- How did it happen?
- When did it happen?
- Is it still happening?
- Who did it happen to?
- What was accessed/acquired? (What wasn't?)

NOTICE OBLIGATIONS

## NOTIFICATION

PROCESS
- Written
- Electronic
- Substitute
- To Media

VENDORS
- Printing, Mailing and Call Center
- Credit Monitoring

REGULATORY INVESTIGATION

LITIGATION
- Government Entities
- Class Action
- Indemnification

# Best Practice

- Use Counsel to Establish **Privilege**
  - Counsel directs forensics, notice drafting, and other vendors so that, in the event of litigation or regulatory investigation, all documents and communications are not discoverable
  - Guard Attorney-Client Privilege: **do not** share forensic reports, legal analysis and drafts with clients or third parties if not absolutely necessary
- Do not **use terms "Breach" or "PII" or "PHI" lightly** — these are statutorily defined legal terms the use and admission of which have consequences
- Do **not rush** to go public
  - Tremendous desire to go public fast, but an inability to answer questions that will inevitably follow can be devastating
  - **If you notice goes out 4 hours after discovery, there will be people who charge you with delay, so "delay" is unavoidable**
- **Prepare for litigation** and regulatory investigation — Preserve all relevant documents
- Conduct **risk assessment** and implement **data security improvements** prior to being asked by a regulator