WHAT DO CISOS DO ALL DAY?

FEBRUARY 2018
GOALS

• Increase familiarity with ICE

• Introduce the challenges in Critical Financial Infrastructure security

• Introduce the Threat Objective-led strategy

• Overview a department/roles organized around Threat Objectives

• Challenge some popular but harmful security misconceptions

• Share some non-obvious defensive tricks
INTERCONTINENTAL EXCHANGE: A STORY OF GROWTH AND INNOVATION

2014
ICE acquires Singapore Mercantile Exchange and SuperDerivatives, announcing Pidglen Clearing House investment, expanding clearing and risk management globally.

2013
ICE acquires majority stake in APM Eurex and launches ICE Eurex, a continental European energy exchange.

2009
ICE launches two CDS clearinghouses, quickly becoming the global leader.

2008
NSYE Euronext acquires the American Stock Exchange (AMEX).

2007
NYSE Group merges with Euronext, creating the first trans-Atlantic stock exchange.

2006
NGS and Archipelago merge, creating NYSE Arca and forming the public entity, for-profit NYSE Group.

2001
ICE extends into energy futures by acquiring the International Petroleum Exchange.

2000
ICE introduces its first cleared OTC energy contracts; LIFFE is acquired by Euronext.

1997
Continental Power Exchange (CPEX) acquired to build new electronic OTC energy marketplace.

1982
The London International Financial Futures and Options Exchange (LIFFE) is established to trade short-term interest rate derivatives.

1977
Twenty-four brokers sign the Butterfley Agreement outside of 68 Wall Street in New York to begin trading securities.

MIX

100% Revenues of $1.5bn
- 50% Derivatives
- 14% Other
- 13% Market Data
- 11% Listings
- 6% Cash Equities Trading

- 2004: ICE Clear Europe
- 2000: ICE Clear Canada
- 1999: ICE Clear Credit
- 1998: The Clearing Corporation

CENTRAL CLEARING HOUSES
ICE Clear U.S.
ICE Clear Europe
ICE Clear Canada
ICE Clear Credit
The Clearing Corporation

LISTINGS LEADERSHIP
Global leader in NYSE capital raising with $83 billion in capital
Leader in total IPOs and technology IPOs
Home to 98% of the DJIA and 78% of S&P 500 companies.

CENTRAL CLEARING HOUSES
ICE CME Group
ICE CME Group
ICE CME Group
ICE CME Group
ICE CME Group

CASH EXCHANGES
New York Stock Exchange
NYSE
NYSE Arca
NYSE MKT
NYSE Arca Options
NYSE Arca Options

FUTURES EXCHANGES
ICE Futures U.S.
ICE Futures Europe
ICE Futures Canada
ICE Eurex
Liffe

MARKETS & CLEARING
PRODUCTS

TRADE EXECUTION
Operates the leading and most liquid group of equities and equity options exchanges.
Hosts the majority of the world’s traded crude and refined oil futures contract volume.
Home to the most liquid market for short-term European interest rates benchmarks in interest rates, energy, equity, FX & equity indices.

CENTRAL CLEARING
5+ million futures and OTC contracts cleared daily.
1st to offer clearing in the OTC energy and credit markets.
The world’s leading clearing of energy futures & credit default swaps.

GLOBAL FINANCIAL MARKETS INFRASTRUCTURE

11
Exchanges
12,000+
Listed contracts
and securities
15.3
million in trade volume each day
$28
trillion market cap
of NYSE listed companies

INTERCONTINENTAL EXCHANGE
NYSE Euronext
ICE
SMX
Apex
Hedge
American
European
ICE
IPE
CME
GLOBEX
ICE

www.ice.com
THE CHALLENGE - CRITICAL FINANCIAL INFRASTRUCTURE

- Critical mission
- Heavy regulation and governmental attention
- Highly motivated/involved Board and Senior Management
- Peacetime/Wartime challenge
- Major media cybersecurity buzz
- Vendor fear peddling
- Finite resources – at any budget level
ENTERPRISE STRUCTURE/ROLES

Cybersecurity
- Digital Forensics & Incident Response / SOC
- Threat Intelligence
- Cyber Fraud
- Architecture
  - Network Monitoring
  - Insider Threat / Behavioral
  - Automation & Analytics

Security Assurance
- Application Security
- Red Team
- Governance, Risk, and Compliance
  - IAM
  - Risk Assessment
  - Third-party/Vendor Assessment
  - Program Defense/Description
  - Policy

Management
- All of the above
- Decision Making
- Strategy
- Creating the Rules
- Diplomacy

Staff Allocation
- Cybersecurity
- AppSec
- RedTeam
- GRC
- Management
THREAT OBJECTIVE-DRIVEN STRATEGY

- **CyberGov**
  - Validates Threat Objectives

- **Blue Team**
  - Prevents, detects, and improves

- **Red Team**
  - Constructs and executes tests

- **GRC**
  - Tracks remediation
  - Scores residual risk
THREAT OBJECTIVES (EXAMPLE SCORES)

- AT: Asset Theft
- NT: NPMI Theft
- PII: Personally Identifiable Information
- EX: Extortion
- FF: Financial Fraud
- ES: Economic Sabotage
- CM: Commodity Malware
- CD: Customer Data Theft
- IP: Intellectual Property

Residual Risk: Destructive attacks to undermine confidence in financial markets
Inherent Risk: DDOS or Ransomware Extortion

Threat Objectives

- Economic Sabotage: Destructive attacks to undermine confidence in financial markets
- Asset Theft: Cyber enabled theft of assets
- Extortion: DDOS or Ransomware Extortion
- NPMI Theft: Trading ahead of M&A or earnings-type data
- Commodity Malware: Recruiting servers to use for non-ICE missions
- Financial Fraud: Stealing credit cards or wire transfer fraud
- Personally Identifiable Information: Stealing employee or customer identifiers (Identity Theft)
- Data Manipulation: Malicious alteration of data (e.g. index, benchmark, or settlement) for financial benefit
- Customer Data Theft: Position data theft for reputational harm or profit
- IP Theft: Stealing ICE Intellectual Property
# THREAT OBJECTIVE CALCULUS

<table>
<thead>
<tr>
<th>Impact</th>
<th>Inherent</th>
<th>Residual</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reflects current and future <strong>business profile</strong></td>
<td><strong>Red Team validation of segmentation controls</strong></td>
</tr>
</tbody>
</table>

## Likelihood

### Inherent

- **Threat Intelligence**
  - Red Team validation of preventative and detective **controls**
  - Known **vulnerabilities**
  - Cultural **risks**
POPOPULAR MISCONCEPTIONS

CHASING PHANTOM MENACES CONSUMES LEGITIMATE RESOURCES

• Patching protected you from WannaCry.
• Inconvenience and security are directly correlated.
• Password complexity is the best defense against brute force attacks (versus offline cracking).
• “80% of breaches.. leveraged (stolen and/or) weak passwords” (Verizon DBIR 2017)
• End-to-end encryption is a reasonable control for enterprise email
• You will get an accurate CMDB or network diagrams.
• Proxies and jump-boxes prevent compromise.
• Endpoint security is the best place to invest in technology
• You can block github
• Network segmentation is impossible
DEFENSIVE TRICKS

UNSUSTAINABLE CONTROLS THAT WILL ONLY WORK 90% OF THE TIME

• gTLD blocking - .ru, .biz, .info
• Web crust egress
• Lateral desktop firewall controls – poor man's network segmentation
• Zero staff 1FA outside the perimeter
• #whoami
• VIP spoof and encrypted attachment quarantining
• Employee scoring and comp haircuts
• Buy v. build? Builders buying