

The ACLI logo is located in the top right corner. It consists of three slanted parallel lines followed by the letters "ACLI" in a bold, sans-serif font.

ACLI

drive▶▶

ACLI Annual Conference 2019

October 13-15 | Sheraton Boston Hotel | Boston, MA

Legal/Compliance: The Financial Crime Landscape

Evolving Financial Crime Threats in a Digital
World



Andrew Davies

VP, Global Market Strategy, Financial Crime
Risk Management
Fiserv

///ACLI

drive▶▶



Timothy Hartmann

Head of Technology Strategy - Compliance
Manulife

///ACLI

drive▶▶

The Financial Crime Landscape

Evolving Financial Crime Threats in a Digital World

///ACLI

drive▶▶



Evolving Financial Services Landscape

The World Is Changing – Pace Is Accelerating



Transactions

- Days, weeks
- Customer service
- Transactions
- Multistep
- Physical location



Integration

- Next day
- Self-service
- Pay online, mobile
- Contactless
- Regulation
- Cyber security
- Social media



Simple digital experience

- Instant, real time
- Customer experience
- One-click
- Biometrics
- Tokenization
- Card-free
- AI
- IoT / IoE

Real-World Challenges Financial Institutions Are Facing



High Overhead Costs



Too Many Demands for Attention



Rapidly Changing Environment



Better Bad Guys with Better Financing



Mandatory Compliance and Reporting Requirements



Inability to Provide Timely and Appropriate Responses to Breaches

Regulator Priorities in 2019

- Matters of importance to retail customers of financial institutions, including seniors and those saving for retirement
- RegTech – Innovation in regulatory compliance
- Anti-Money Laundering
- Compliance and risk in registrants responsible for critical market infrastructure
- Digital Assets
- Cybersecurity
- Compliance with FinCEN's Customer Due Diligence rule will look at customer identification procedures and suspicious activity monitoring for accounts opened to transact in crypto
- Seven of the top ten largest fines in the FCPA's history have been imposed in the last five years



Evolving Threat Landscape

New Threats Are Emerging Everyday

more costly and complex than ever with no slow down in sight

\$2.4 average cost of
malware attack
Million

1.5M
Shortfall in
Cybersecurity talent

4.2 Billion
Records breached
in past year

\$5.1B
Account Takeover Fraud
3X Growth

80% of financial crime
schemes are driven
by **organized crime**

300 Billion
passwords in use by 2020

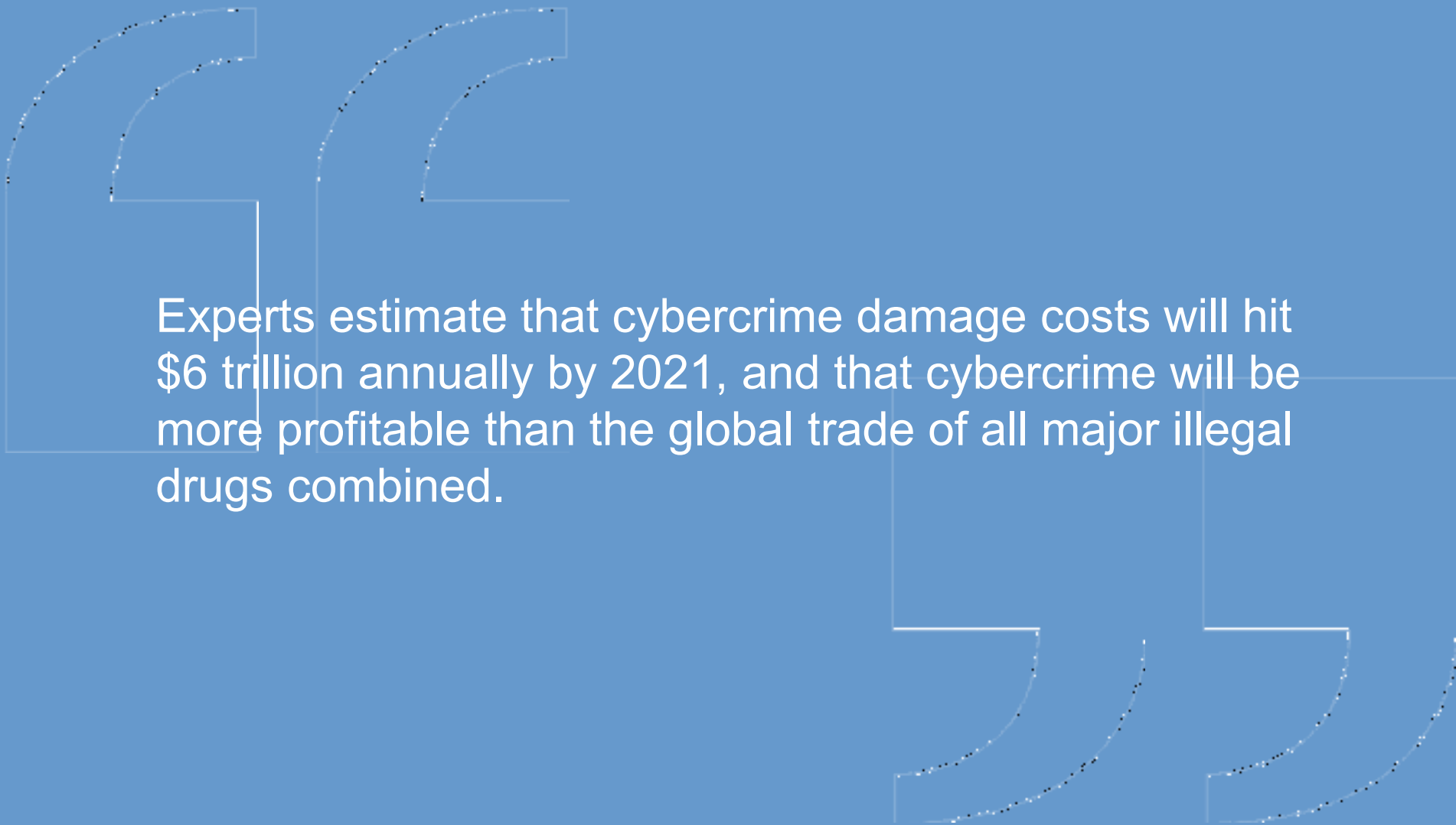
\$6 Trillion
Cybercrime damage annually by
2021

\$3.6 Trillion
Money laundered through
global financial systems

**Ransomware
attacks every**
14 seconds

68%
of financial institutions
took months to
discover breaches

\$321 Billion
Anti-Money Laundering Fines
16.7M ID Theft Victims
highest on record



Experts estimate that cybercrime damage costs will hit \$6 trillion annually by 2021, and that cybercrime will be more profitable than the global trade of all major illegal drugs combined.

Today's Threat Landscape



Targets

68% of financial institutions took months or longer to discover breaches

58% of breach victims were smaller institutions

80% of financial institutions replaced or augmented their existing AV solutions



Threat Actors

73% of breaches are perpetrated by outsiders

60% of breaches are conducted by organized crime

92% of breaches originated through email



Tools

21% decrease in executables in favor of evasive, file-less techniques

87% of compromises took minutes to execute

37% of malware hashes only appeared once

Verizon Breach Report 2018

Real-World Targeting of Financial Institutions



The Numbers Are Rising

29,839

Compromised
employee credentials
from 3rd party leaks

937,000

Targeting by threat
actors in last 6 months

6,646

Mentions on dark web
forums in the last 6 months

110,000

Potential brute-force
login attempts

2,200

Unique threat
actor usernames

Advanced Malware beating Traditional Defenses

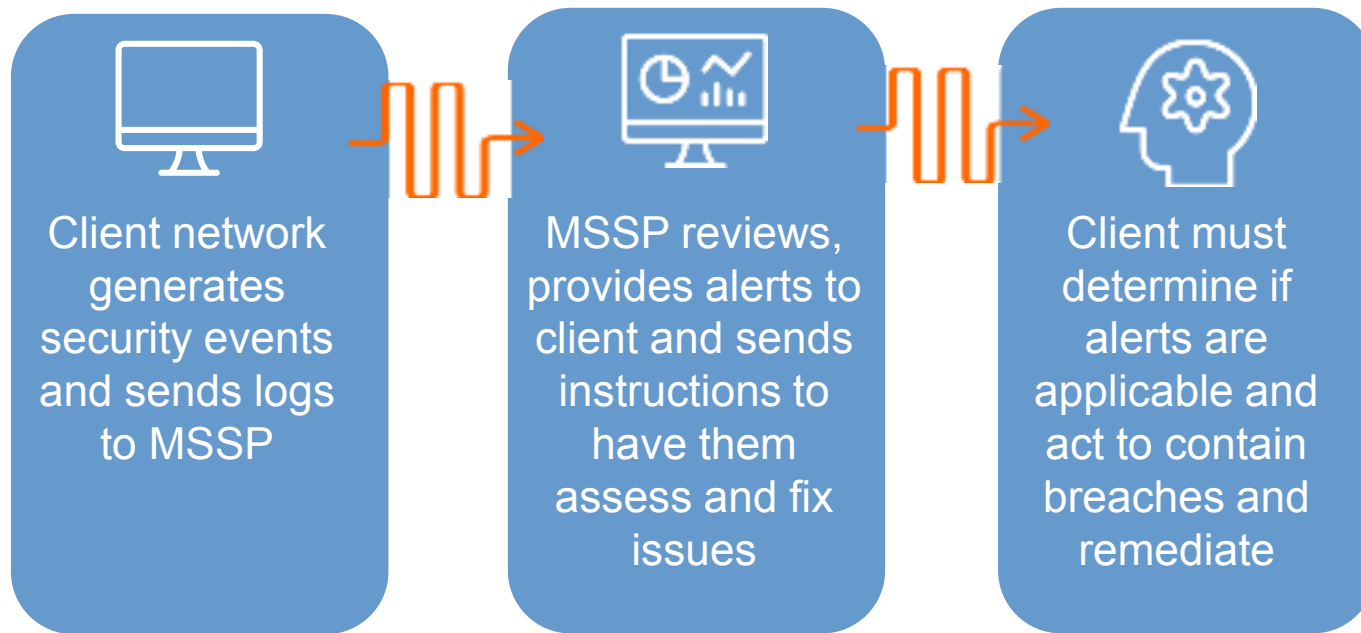
- File-less advanced malware that mutates to avoid detection by standard anti-virus
- Steals banking details and passwords

Polymorphic Malware
Accounted for **57%**
of all banking trojan
payloads in Q1 2018*

* Proofpoint Q1 2018 Threat Report

Legacy Security Operations Are Not Enough

Siloed Detection, Instructional Response, Inadequate Remediation



Why are they not enough?

- Defenses not integrated
- Alerts not prioritized & causing alert fatigue
- No follow-through on alerts to remediation
- Limited access to sophisticated and actionable external threat intelligence resources

Recent Trends in AML: FATF's Revised Guidance on the Risk-Based Approach for the Life Insurance Sector

Why the revision?

- Reflect changes (e.g., tax evasion added as predicate crime) since 2009 Guidance
- ML/TF Risk Assessment is a key starting point
- Confirming expectations (SARs are not risk based)
- Enhance guidance to provide examples of risk factors

Audience

- Governments
- Supervisors
- Insurers and Intermediaries

Key Themes

- Assessment design is commensurate with insurer's risk & complexity
- Reliance and involvement of intermediaries
- Ranking risk and mitigation measures to determine residual risk
- Tone from the top and three lines of defense model

Top 10 ways to Quantify & Manage Financial Crime Risk

Approach #1

Risk Assessment – Product Profile and Risk



Approach #2

Customer Centric View



Approach #3

Omni Channel Monitoring



Approach #4

Collaboration & Training



Approach #5

Data Management



Approach #6

Leverage Robotics



Approach #7

Leverage Analytics and Machine Learning



Approach #8

Business Intelligence and Reporting – Financial Tracking



Approach #9

Fine Tuning - Risk Assessment



Approach #10

Monitor Red Flags



Fraudulent Account Takeover Red Flags

- Loan request short time after registering policy with online portal
- Loan request short time after address change
- Loan request directing funds to be wired or ACH'd to new bank account, not bank account of record
- Loan request directing funds be mailed to new address, not address of record (e.g., hotel, vacant home) or a P.O. box
- Loan request directing funds to be wired or ACH'd to newly established bank account
- Irregular signatures on loan request
- Use of VOIP phone number when calling
- Urgency of transaction
- Calls to call center in which voice is distorted, caller mispronounces words, or pii of customer is not readily available
- Email requests which contain poor grammar, unusual font, or poor syntax
- Requests which indicate that the policy/account holder is traveling/unavailable/unreachable
- Use of free email services which do not require any personal information or verification to establish account (e.g., mail.com, homemail.com)

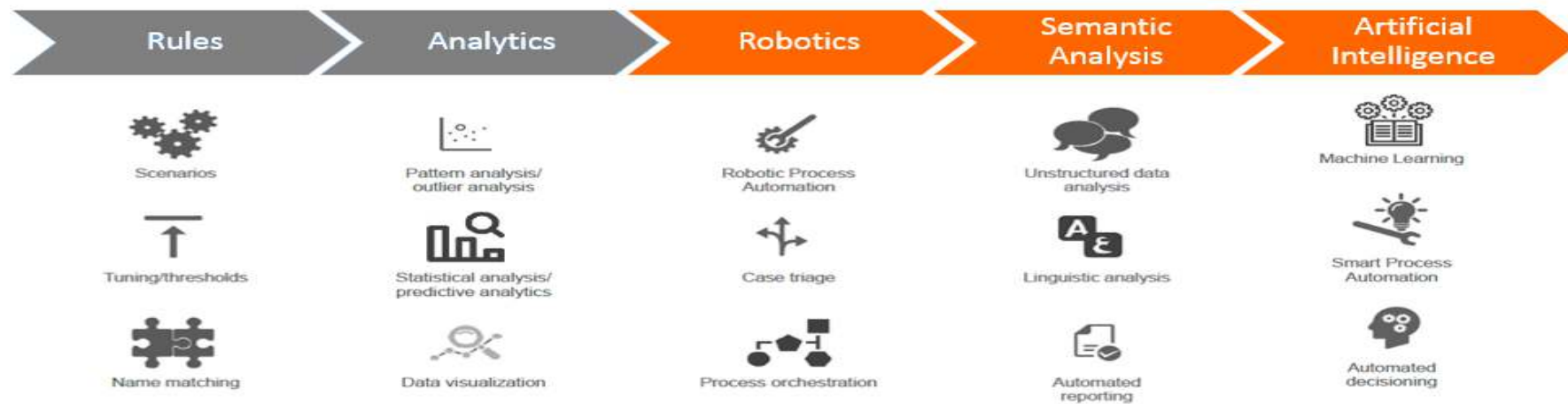
Money Laundering Red Flags

- Premiums being paid into one policy, from different sources
- Making over-payment on a policy, then asking for a refund
- Unusual relationship between policyholder and beneficiary
- Channelling payments via offshore banks
- Funds coming from another country, particularly a high-risk jurisdiction
- Customer wants to pay a large premium with foreign currency
- Application for a policy from a potential client in a distant place where a comparable policy could be provided “closer to home”
- Insurance policy premium exceeds the client’s apparent means
- Transactions involving an undisclosed party
- Early termination of a product, especially at a loss, or where cash was tendered and/or the refund check is to a third party
- Applicant shows little concern for policy performance, but much interest in early cancellation provision
- Information provided by the customer that identifies a legitimate source of funds is false or misleading
- Upon request, customer refuses to identify or fails to indicate any legitimate source for his/her funds and other assets
- Customer or associated person has a questionable background or is the subject of new reports indicating possible criminal, civil, or regulatory violations
- Customer requests that a transaction be processed in such a manner to avoid the firm’s normal documentation requirements



Evolving Technology to Manage Risk

Shift Towards Next Generation Solutions



Source: Celent 2018

Technology Driving Next- Generation Solutions

Advanced Analytics



Data Mining
Statistical Analysis
Predictive Analysis
Link Analysis

Often employing
specialized open
source or
proprietary
modeling
languages

Software Robotics



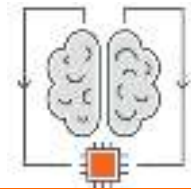
Robotic process
automation (RPA)
to handle routine
processes and
smart process
automation (SPA)
that joins robotics
with artificial
intelligence to
enable the
automation of
workflow tasks
that require
decisions

Semantic Analysis



Unstructured data
in texts, images,
and audio to
greatly expand the
data universe
susceptible to
meaningful
analysis

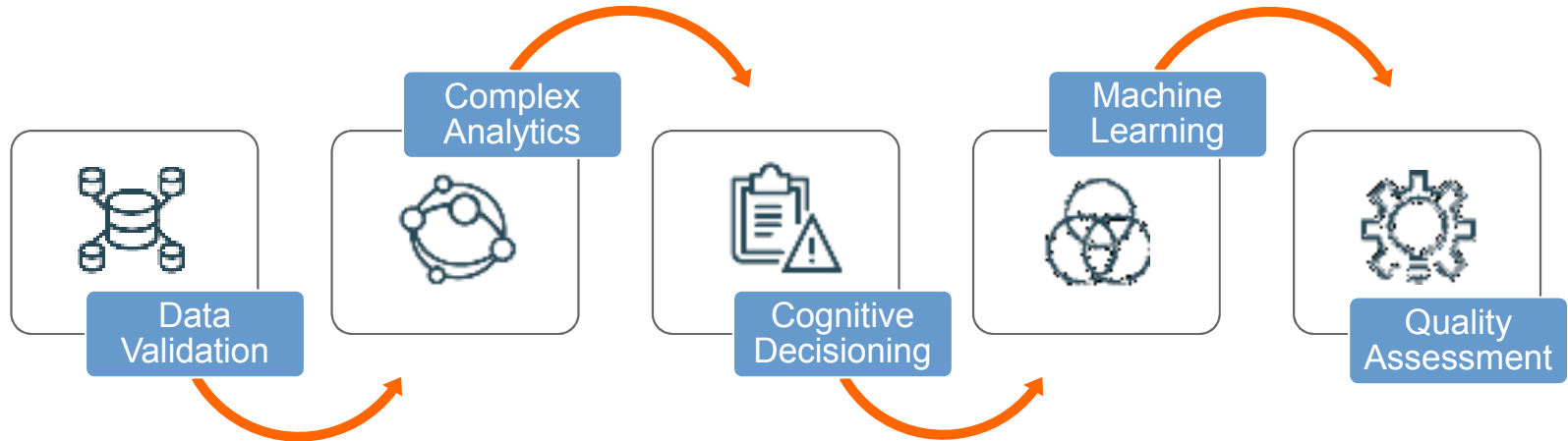
Artificial Intelligence



Which utilizes
multiple
technologies to
imbue computer
systems with
some of the
cognitive and
decision-making
faculties of
humans.

Source: Celent 2018

AI, ML, NLP: How & where to apply?



Three Key Takeaways

1 Impact of the transformation of financial services on risk

Understand how the global transformation of financial services introduces new financial crime risks and trends

2 Leverage a risk based approach

Understand the need to focus on a risk based approach to managing financial crime risk based on your institution's risk profile and how this impacts customer experience

3 Leverage technology

Understand how technology can help manage financial crime risk given the brave new world that we live in.



Questions