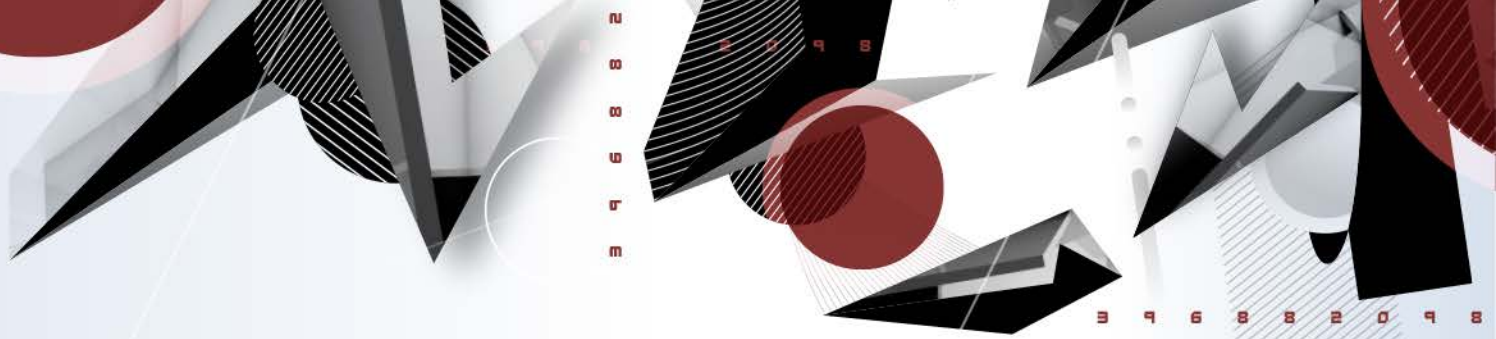


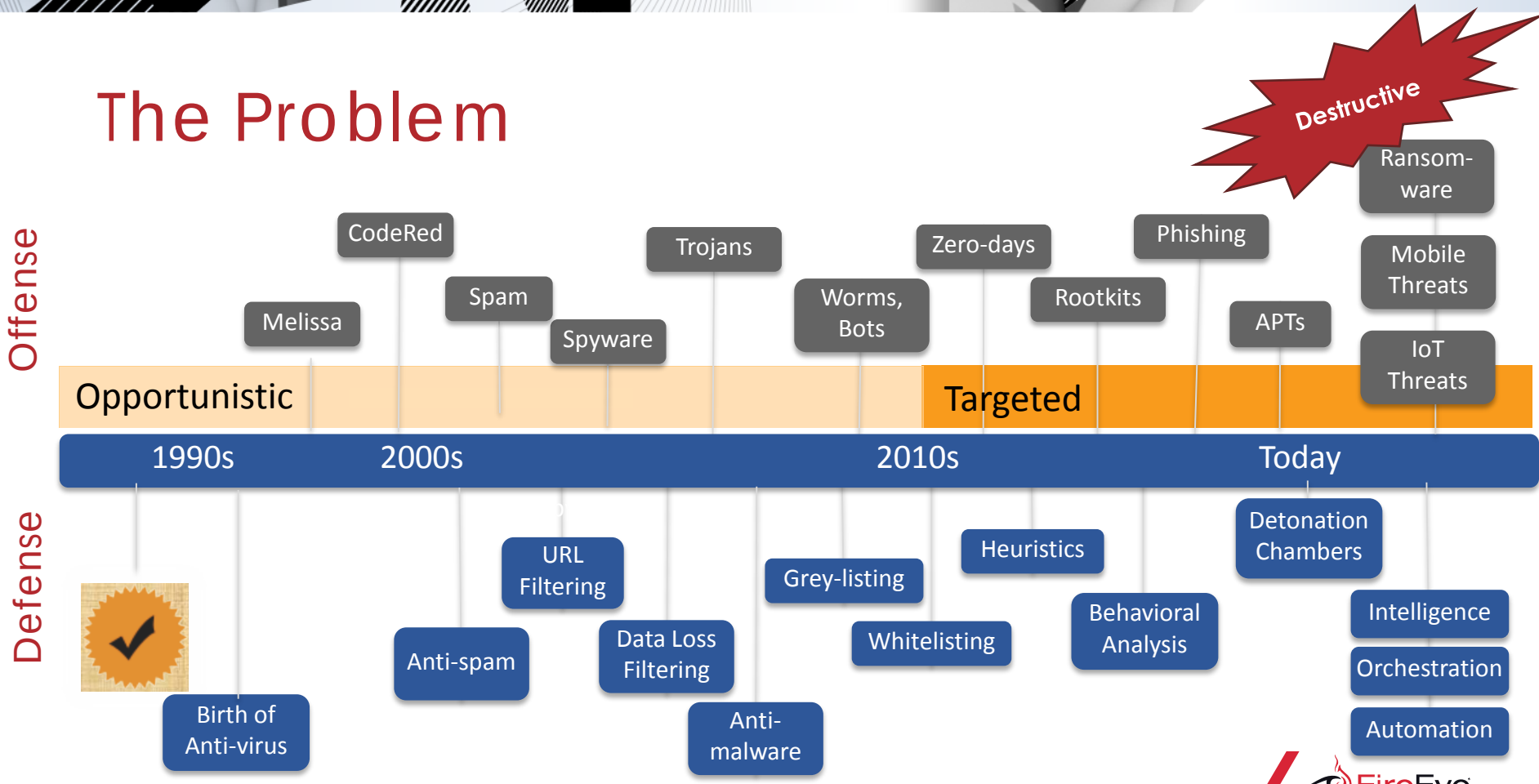
FireEye

Systemic Cyber Risk and Exposure of the Insurance Industry

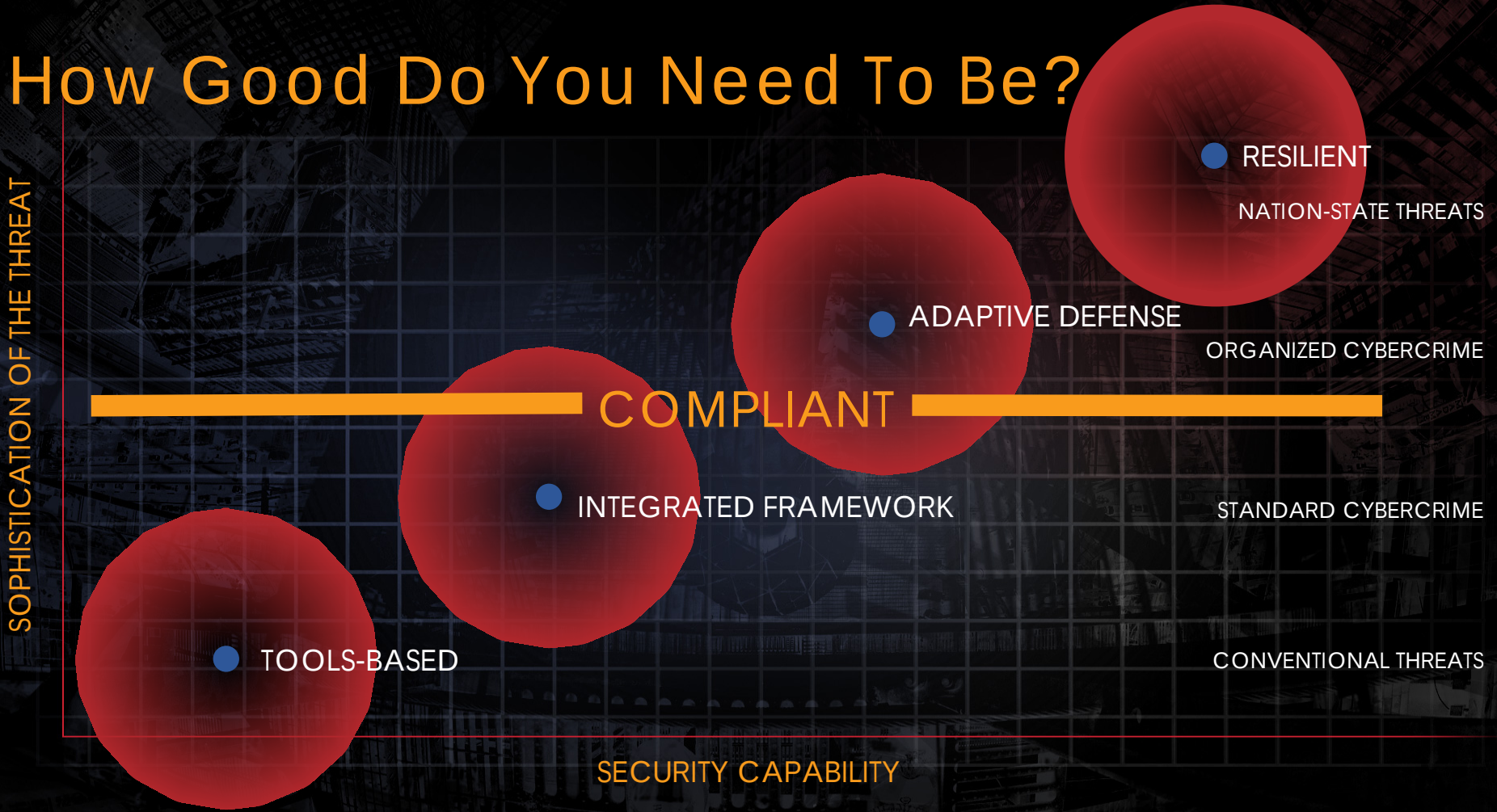
Ron Bushar, VP, FireEye Professional Services

Christopher Porter, Chief Intelligent Strategist

The Problem

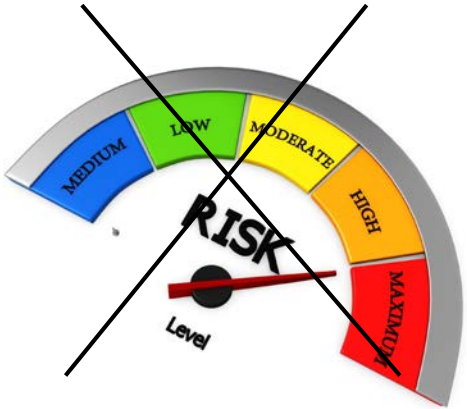


How Good Do You Need To Be?

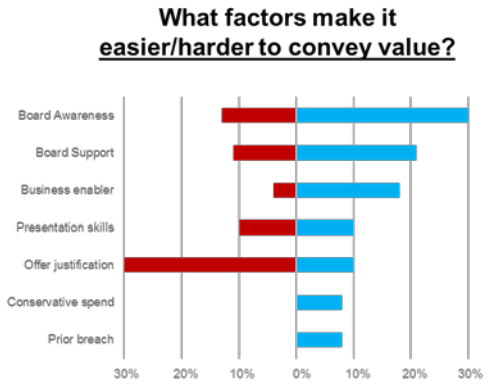


Background: Why **Cybersecurity Risk Management?**

Old methods don't work



Need to engage at Board-level



Source:
Cyber Balance Sheet - https://focal-point.com/insights/cyber-balance-sheet

Rapid growth in cyber insurance market

$14B

Expectation globally, by 2022, a 28% CAGR from 2016 – 2022.

Source:
https://www.alliedmarketresearch.com/press-release/cyber-insurance-market.html

Risk Services Objectives

- Help the CISO / CIO communicate business risk at the Board-level.
- Help client security operations use risk management techniques in practice.
- How do you communicate the scale of the risk to stakeholders across the team?
- What organizational steps does your team use to reduce risk?
  - Examples - mapping key assets and putting contingency plans in place.
- How can you financially transfer these risks?

Intelligence-led security is about **risk management**

- What should organizations be doing to benefit from intelligence-led security?
- Companies need real-time adversary analysis **before** an incident.
- Understanding the risks, what informational assets (and asset value) an organization has, and where those assets are located.
- Who at the company is responsibility for assessing and mitigating breach-related risks? Not just the chief information security officer (CISO).
- Cyber Team should consist of internal stakeholders as well as outside partners like law firms, insurance experts & Forensic teams like Mandiant.

Defining your risk impact **across the organization**

Cyber is not just an IT issue.

It is an **enterprise risk** that impacts many key stakeholders within your organization.

Where should I start?

- Incident response plans?
- Has your team done a table-top exercise?
  - Both technical & executives should participate.
- Practice and include your outside partners.
  - This is a working document, so update the plan after practice.
- Once you've identified gaps, create action plans to eliminate them.

Breach Response Hot Topics

- Having a communications playbook
- Dealing with Brian Krebs
- The right mitigation product (credit monitoring and others)
- The “b” word
- Notification timelines & expectations
- Your plans (not just Incident Response plans)
- Breach response goals vs. risks

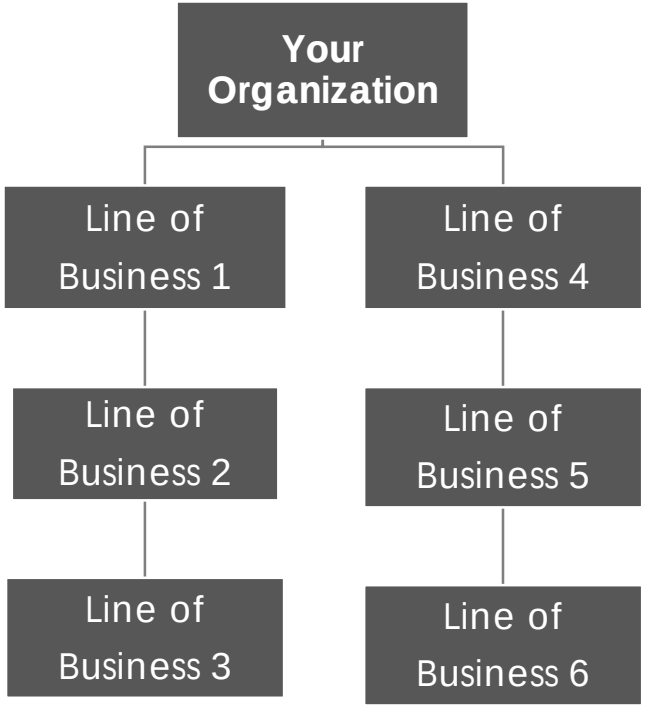
Achieve Resilience by focusing on the "Relevant Threats"; "Buy Down" Cybersecurity Risk by Optimizing Investment in Countermeasures

How does the adversary view your organization?

Optimize decision-making with risk-led security

Identify & Track the "Relevant Threats"

Use threat diagnostics or iSight Intelligence to inform and guide.



Measure Business Risk and Plan Investments

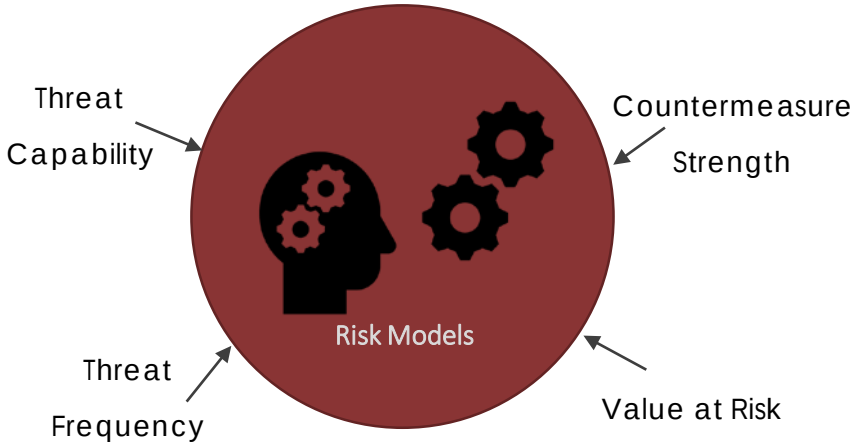
Old Method

Reliable measures of risk cannot be derived from a simple equation…

~~Probability x Impact x Vulnerability = Risk~~

New Method

Optimize by relying on risk models appropriate to your organization. Allow for inclusion of multiple risk factors.

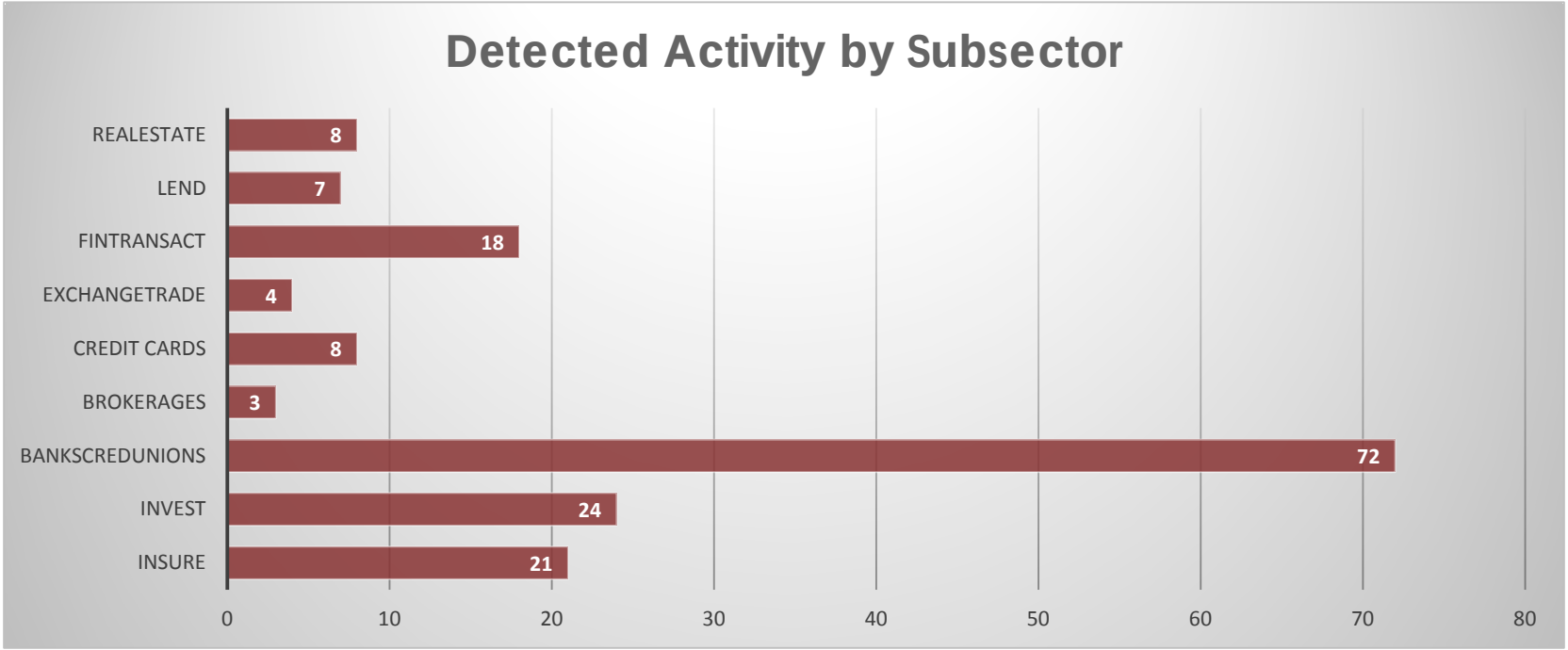


2018

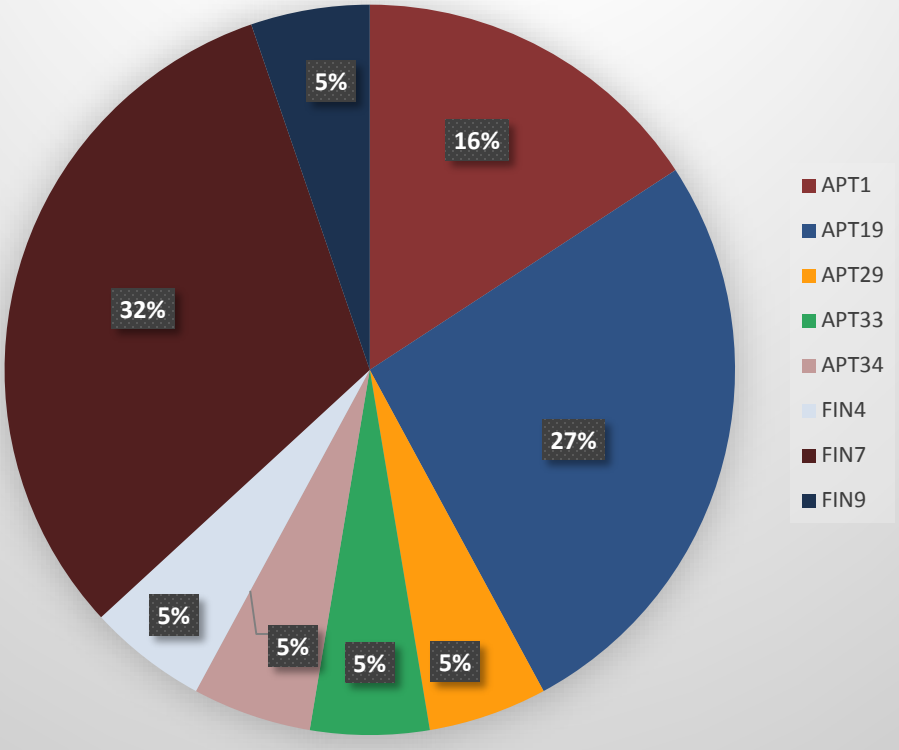
and beyond...

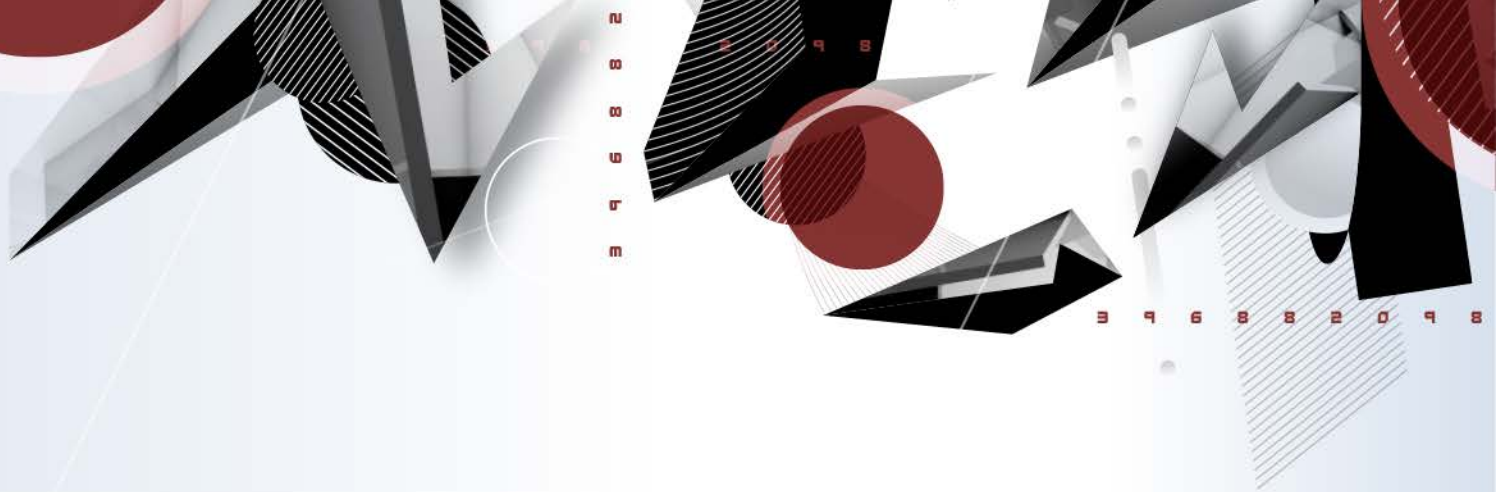
- More destructive attacks
- Attribution will become more important
- Attacks will continue to align with global conflicts
- More reliance on cloud infrastructure (both victims and attackers)
- Cyber security will continue to be a national focus
- More and more sophisticated threat actors will emerge
- More government involvement
- Intelligence and sharing are critical to stay ahead of the threats
- Attacks against safety control systems

Insurance a Top Finance-sector Target



Investment Targeting by Actor





FireEye

Thank you.

We look forward to working with you.