FireEye Cyber Trendscape - 2020

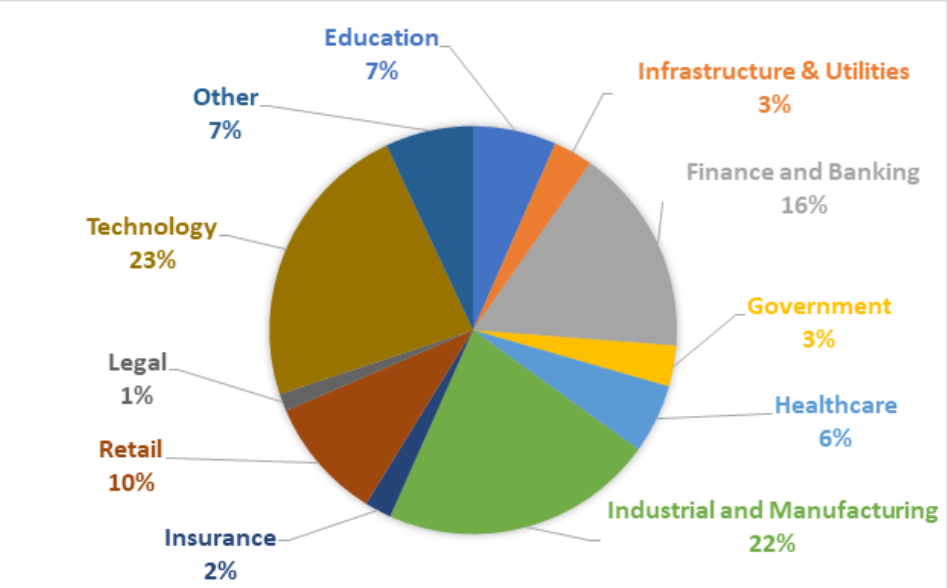
EXCLUSIVE PREVIEW

Eric Ouellet
Global Security Strategist

Cyber Trendscape - Executive Perspectives

Large-scale cyber security research initiative:

- 800 senior Executives
- North America (US and Canada), Europe (France, Germany and the UK), Asia (China, Japan and South Korea)



Cyber Trendscape - Executive Perspectives

Broad Range of Cyber Security Topics

- Balancing Cyber Security and Operations
- Cyber Security Budgets
- Organizational Maturity and Resilience to Cyber Threats
- Security Program Maturity
- Response Plans
- Cyber Security Insurance
- Security Operations
- Threat Intelligence
- Artificial Intelligence
- Block Chain
- And much more !

While there were regional nuances with the findings participating organizations were remarkably consistent in their views and perspectives of cyber security

Panelists

- **Michael Bower** – CISO, Celanese
- **Eric Ouellet** (Host) – FireEye Global Security Strategist

Cyber Trendscape - Executive Perspectives

- Security Priorities, Initiatives and Budgets
- Maturity and Resilience to Cyber-Threats
- Security Operations
- Key Trends and Take Aways

Key Finding – Threat Landscape

- Over 90% of organizations believe cyber threats will stay the same or worsen in 2020

- The top three industry sectors believed to be the most likely targets of a cyber attack are:

  Finance and banking

  Technology

  Government

Key Finding – Operations vs Security

- Finding a balance between cyber security and operational requirements is a challenge for 63% of organizations.

Key Finding – Security Budgets

- 76% of organizations are planning cyber security budget increases for 2020
- Most plan increases of 1-9% over the current 2019
- 2019 cyber security budget averages 6-7% of the overall IT budget

Key Finding – Security Programs

- 27% of organizations characterize their cyber security program as semi-formal approaches where efforts were mostly compliance driven and focused on addressing mandatory regulations
- 24% saw their programs as informal with a focus is primarily on addressing critical issues as they occur
- Only 19% of organizations identified their security program as strategic with intelligence data driving investment decisions, operational priorities and other critical cyber security factors.

Key Finding – Response Readiness

- Globally, 51% of organizations do not believe they are ready or would respond well to a cyber attack or breach event

- Nearly 29% of organizations who have cyber attack and breach response plans have not tested or updated their plans in 12 or more months

Key Finding - Training

- Over 40% of organizations do not have or have only very limited as-needed cyber security training for their employees

- France with a 67% higher response rate than the global average excluding France, was the only country that believed employee training was the cyber security investment area with the highest potential positive impact to protect their organizations against a cyber attack

Key Finding – Cyber Insurance

- Globally, 50% of organizations reported they had cyber insurance as a complement to their cyber security programs
- A further 41% planning to add it in the next 18 months
- 55% report it is difficult to find cyber insurance
- 46% report cyber insurance provides poor value

Cyber Trendscape - Key Findings

- Full Report Available:

November 11, 2019