Breach Response Preparedness

How C-level Leaders Contribute to a Stronger Security Posture

Executive Playbook Briefing

Stuart McKenzie

Vice President, FireEye Mandiant, EMEA

FireEye Mandiant Security Consulting

Prevent, detect and respond to advanced cyber security events and protect your organization's critical assets.

40%

Trusted by organizations worldwide – **Over 40%** of Fortune 100 companies[1]

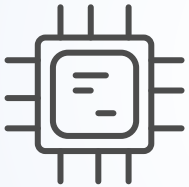
15+

15+ years responding to and remediating headline breaches

Mandiant DNA – Pioneers in sophisticated incident response

Portfolio of services to **assess, enhance and transform** security posture and upskill internal security staff

Cutting-edge **threat intelligence** informed by frontline adversary exposure



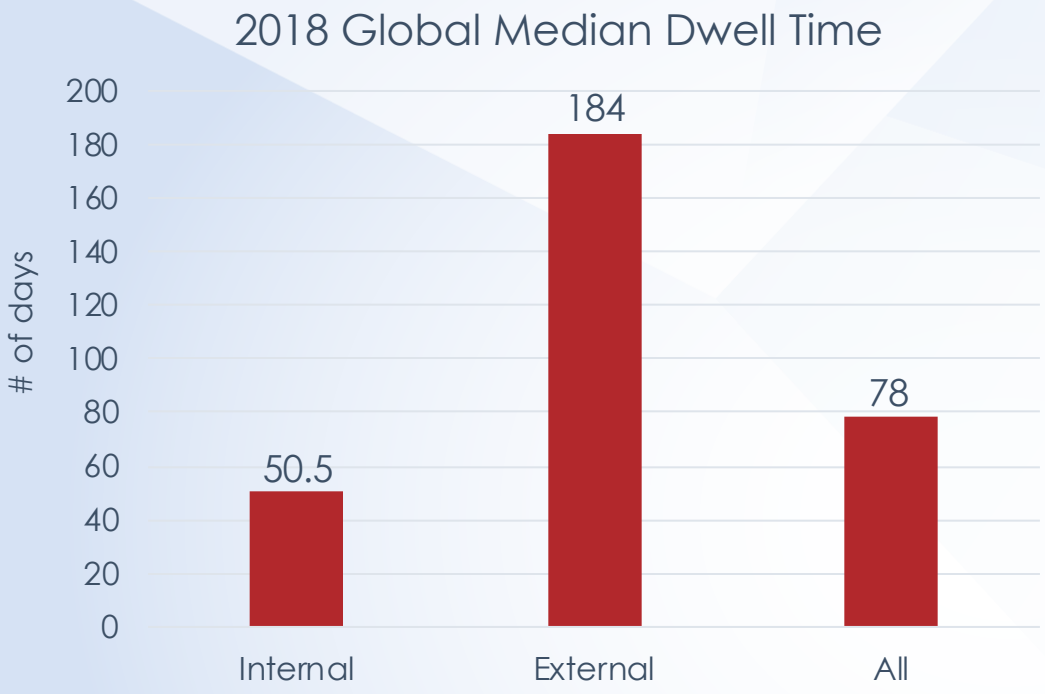
Cyber security services enabled by **purpose-built technology**

Global workforce of over 300 consultants in 20+ countries

Industry-recognized LEADER

- 2019 Forrester Wave: Cybersecurity IR
- 2018 Forrester Wave: External Threat Intel
- 2018 IDC: U.S. Incident Readiness, Response and Resiliency
- 2018 IDC: Asia Pacific Threat Lifecycle Services

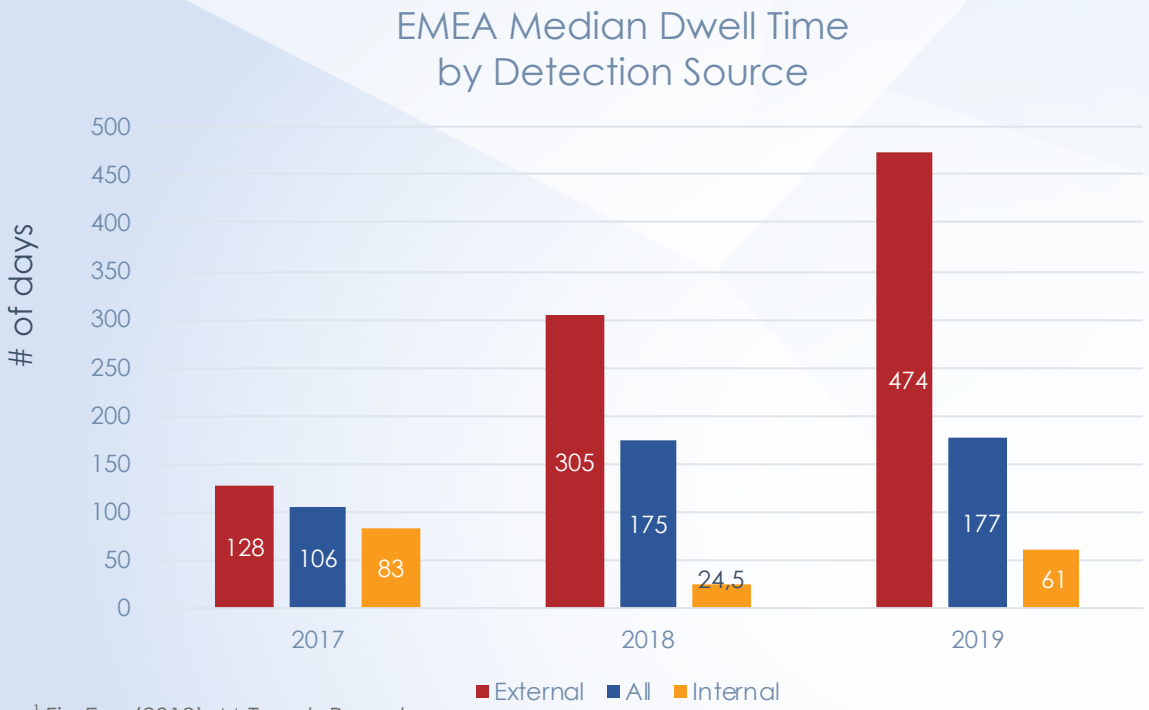
Current State



- In 2017, the average global cost of a data breach was $4.24 million[1]
- Global median dwell time of an attacker is 78 days – Giving threat actors the ability to evade detection for nearly three months[2]
- Tougher regulations sparked increased exposure to today's security risks (e.g., General Data Protection Regulation)

[1]Ponemon Institute (2018). *Cost of Data Breach Study.*
[2] FireEye (2019). *M-Trends Report.*

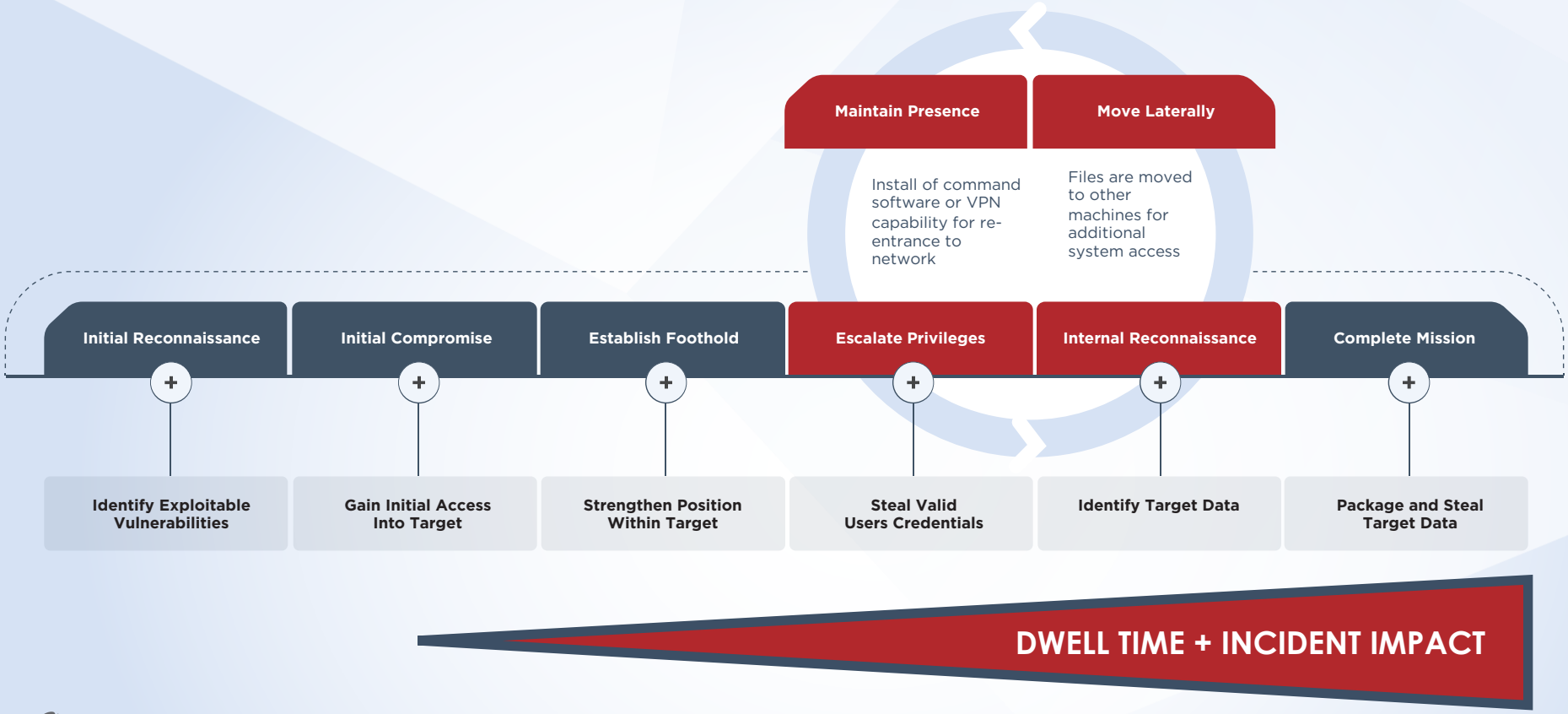
Europe, Middle East & Africa



[1] FireEye (2019). *M-Trends Report.*

- **Significant increase** of median dwell time detection in EMEA
- Detection types have remained at **56% internal and 44% external**
- **GDPR** has driven **positive impact** on cyber hygiene in EMEA

The Attack Lifecycle



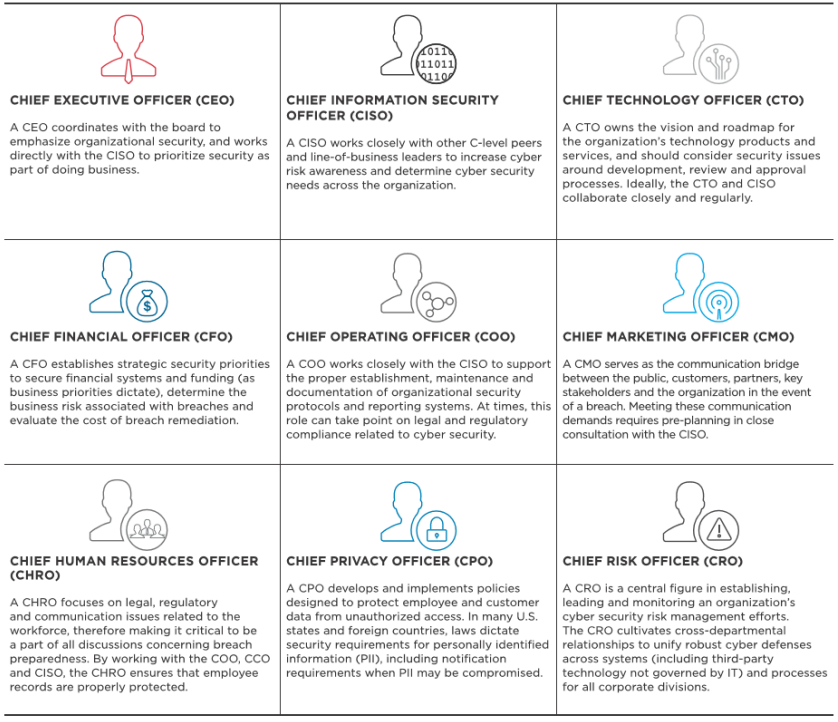
Once a Target, Always a Target

Region	2017	2018
Americas	44%	63%
EMEA	47%	57%
APAC	91%	78%
Global	56%	64%

C-Suite Involvement

Executives are expected to:

- Have knowledge of their organization's security maturity
- Acknowledge understanding of their organization's potential security risks
- Recognize the importance of a proactive incident response plan



CHIEF EXECUTIVE OFFICER (CEO)

A CEO coordinates with the board to emphasize organizational security, and works directly with the CISO to prioritize security as part of doing business.

CHIEF INFORMATION SECURITY OFFICER (CISO)

A CISO works closely with other C-level peers and line-of-business leaders to increase cyber risk awareness and determine cyber security needs across the organization.

CHIEF TECHNOLOGY OFFICER (CTO)

A CTO owns the vision and roadmap for the organization's technology products and services, and should consider security issues around development, review and approval processes. Ideally, the CTO and CISO collaborate closely and regularly.

CHIEF FINANCIAL OFFICER (CFO)

A CFO establishes strategic security priorities to secure financial systems and funding (as business priorities dictate), determine the business risk associated with breaches and evaluate the cost of breach remediation.

CHIEF OPERATING OFFICER (COO)

A COO works closely with the CISO to support the proper establishment, maintenance and documentation of organizational security protocols and reporting systems. At times, this role can take point on legal and regulatory compliance related to cyber security.

CHIEF MARKETING OFFICER (CMO)

A CMO serves as the communication bridge between the public, customers, partners, key stakeholders and the organization in the event of a breach. Meeting these communication demands requires pre-planning in close consultation with the CISO.

CHIEF HUMAN RESOURCES OFFICER (CHRO)

A CHRO focuses on legal, regulatory and communication issues related to the workforce, therefore making it critical to be a part of all discussions concerning breach preparedness. By working with the COO, CCO and CISO, the CHRO ensures that employee records are properly protected.

CHIEF PRIVACY OFFICER (CPO)

A CPO develops and implements policies designed to protect employee and customer data from unauthorized access. In many U.S. states and foreign countries, laws dictate security requirements for personally identified information (PII), including notification requirements when PII may be compromised.

CHIEF RISK OFFICER (CRO)

A CRO is a central figure in establishing, leading and monitoring an organization's cyber security risk management efforts. The CRO cultivates cross-departmental relationships to unify robust cyber defenses across systems (including third-party technology not governed by IT) and processes for all corporate divisions.

The challenge:

Determining if and how their organization is prepared to respond to a breach

A Phased Approach – Before an Incident *(three-pronged)*

1. Assess the current situation

- Evaluate your cyber security strategy
- Perform a threat profile
- Review local and global regulations

- **Regulatory Compliance:** Do our response strategies support applicable regulatory and legal requirements?
- **Staffing:** Is our staff organized properly? And do they clearly understand their roles and responsibilities during an attack?
- **Training:** Does our staff have the training they need to respond effectively and efficiently when an incident occurs?
- **Incident Detection:** Does our organization have the mechanisms in place to rapidly detect an incident?
- **Processes:** Do we have a clear process for rapidly responding to potential data breaches?
- **Technology:** Do we have the necessary hardware and software to respond across the enterprise?

[3] FireEye Mandiant Example (2019).

A Phased Approach – **Before an Incident** *(three-pronged)*

2. Objectively evaluate your IR capabilities

- Evaluate your SOC and IR program status
- Build containment and remediation plans
- Test your capabilities (Tabletop exercises)

A Phased Approach – Before an Incident *(three-pronged)*

3. Select an IR vendor / Establish an IR retainer

- Pinpoint organizational needs and internal resources
- Avoid response delays and reduce impact of breach
- Select retainer offering based on specific needs

Ask these six questions to gauge IR vendor experience and capabilities:

- **Do you have a dedicated IR team? What is their experience?**
- **How many incidents did you respond to in the past year? What types of incidents were they?**
- **What malware analysis capabilities and intelligence resources do you have?**
- **Do you have experience working with law enforcement if the need should arise?**
- **How do you make sure that the attackers are truly gone when you complete an investigation?**
- **What type of service levels do you offer when there is a confirmed incident? How quickly can you provide remote support?**

[3] FireEye Mandiant Example (2019).

A Phased Approach – During an Incident

Crisis communication

- Disclose certain information
- Contact the right parties (consider legal and regulatory partners)
- Align on one united message

"We are aware of reports that a Mandiant employee's social media accounts were compromised…

We immediately began investigating this situation, and took steps to limit further exposure…

Our investigation continues, but thus far, we have found no evidence that FireEye or Mandiant systems were compromised." [3]

[3] FireEye Mandiant Example (2019).

A Phased Approach – After an Incident

Security Needs Framework

Looking for improvements

- Ask "could this have been prevented?"
- Understand the vulnerabilities that were exploited
- Enhance processes and upgrade technology

Near-Term Executive Actions

Gain security practice alignment with your CISO

- Ask questions that offer a clear picture of your security team's approach
- Provide guidance on best practice security strategies

Identify opportunities to advance your security program's maturity

- Increase executive oversight
- Realize prevention techniques
- Improve detection methodologies
- Strengthen crisis management plan

How We Can Help

Key Mandiant Consulting services to help with breach response preparedness:

- *Response Readiness Assessment (RRA)* – Maturity assessment of your security monitoring and response capabilities to stop attackers faster.
- *Incident Response Retainer (IRR)* – Established IR service terms and conditions before a cyber security incident is suspected; significantly reduces response time and impact.

Further information and actionable guidance at your fingertips:

- The Executive's Playbook for Breach Response Preparedness
- RRA Datasheet
- IRR Datasheet

7 Reasons to Have Mandiant on Speed Dial

Thank You

Learn more about Mandiant Consulting at
FireEye.com/services