Tervetuloa / Welcome

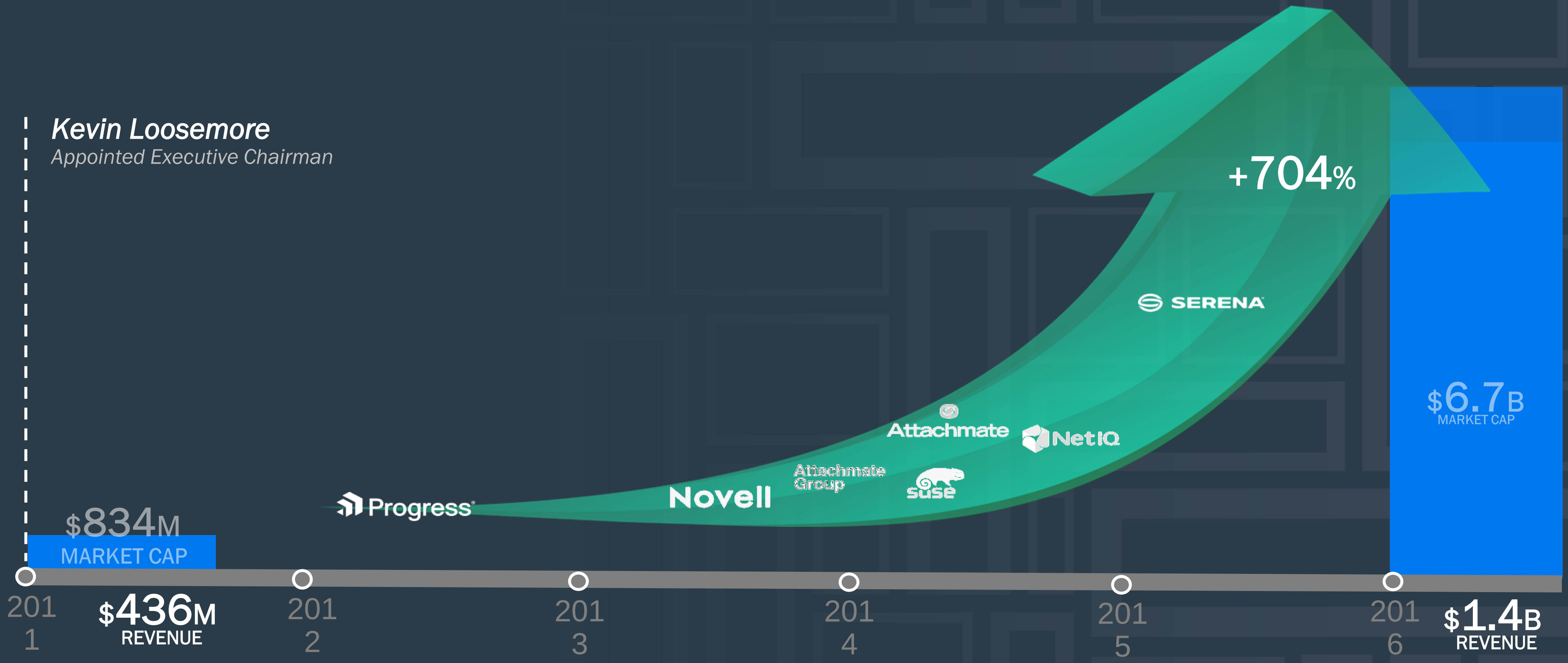
Tim Grieveson
Chief Cyber & Security Strategist – Europe
Micro Focus

Former CIO / CISO / Global Privacy Officer

in https://uk.linkedin.com/in/timgrieveson

@timgrieveson

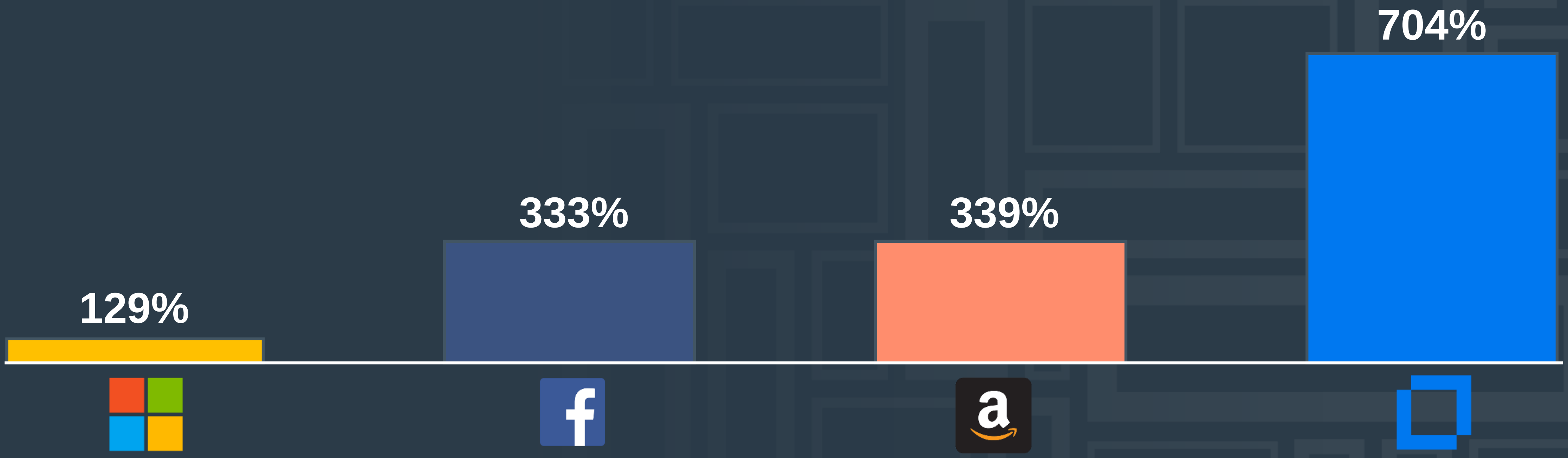
Micro Focus Long-Term Performance



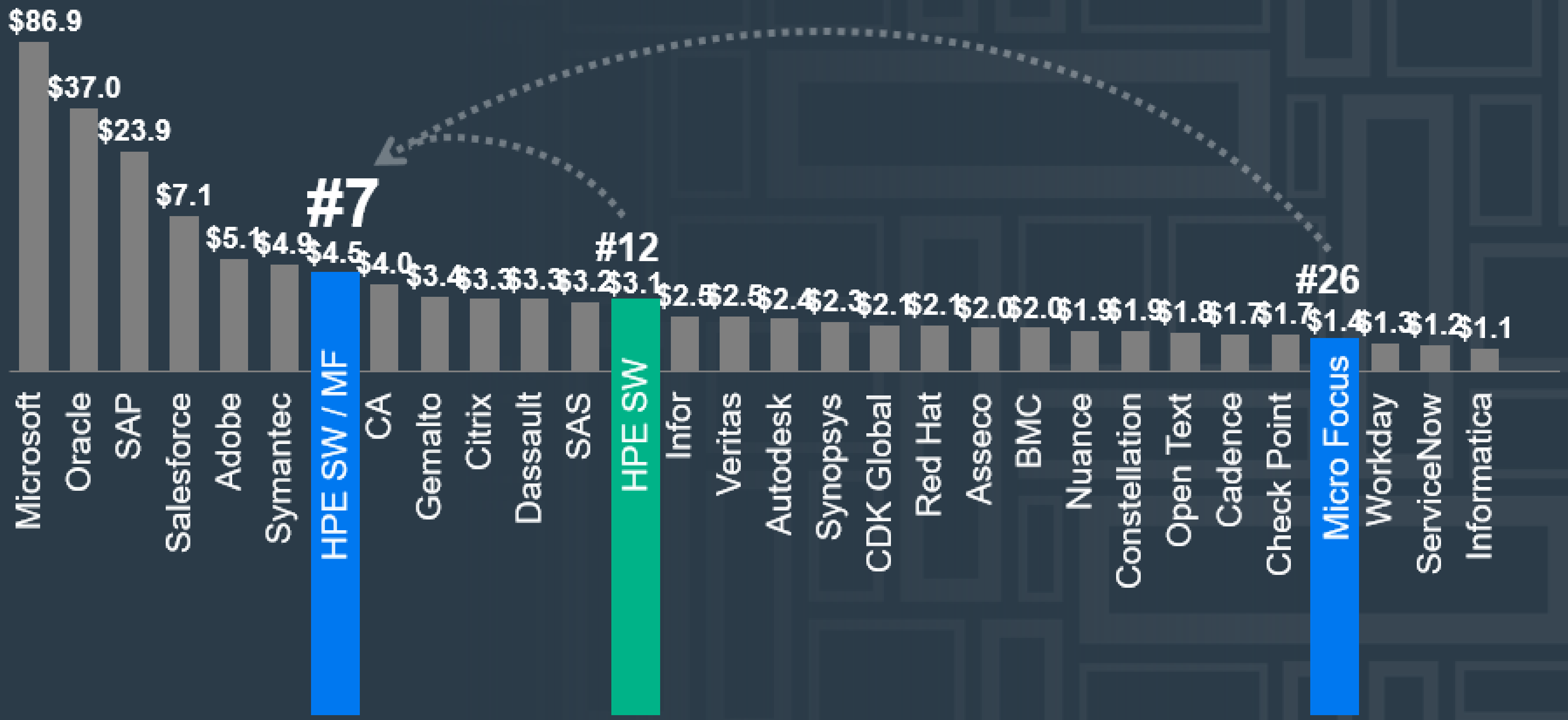
Kevin Loosemore
Appointed Executive Chairman

Micro Focus Market Cap

Under Current Management
Team
2011-2016



Combined Micro Focus: An Industry Shaper



MICRO FOCUS®

“The Internet Of Theft”

Swimming in the Tsunami of Data & GDPR …..
Former CIO / CISO / Global Privacy Officer perspective

Tim Grieveson
Chief Cyber & Security Strategist – Europe
Micro Focus

in https://uk.linkedin.com/in/timgrieveson

@timgrieveson

Know your enemy: The most popular hacking methods

	USA	EU	
1	81%	83%	**SOCIAL ENGINEERING** (e.g. phishing)
2	62%	63%	**COMPROMISED ACCOUNTS**(e.g. weak passwords)
3	51%	54%	**WEB-BASED ATTACKS** (e.g. SQL/command injection)
4	33%	43%	**CLIENT SIDE ATTACKS** (e.g. against doc readers, web browsers)
5	23%	17%	**EXPLOIT AGAINST POPULAR SERVER UPDATES** (e.g. OpenSSL, Heartbleed)
6	21%	16%	**UNMANAGED PERSONAL DEVICES** (e.g. lack of BYOD policy)
7	15%	13%	**PHYSICALINTRUSION**
8	11%	10%	**SHADOW IT** (e.g. users' personal cloud-based services for business purposes)
9	9%	10%	**MANAGING THIRD PARTY SERVICE PROVIDERS** (e.g. outsourced infrastructure)
10	6%	6%	**TAKE ADVANTAGE OF GETTING DATA PUT TO THE CLOUD** (e.g. IAAS, PAAS)

Source: BalaBit.com CSI Report – Feb 2016

Worldwide security trends & implications

Cyber threat

66% compound annual growth rate in number of detected security incidents 2009 to 2014

Extended supply chain

44% of all data breach involved third-party mistakes

Financial loss

$7.7M mean annualized cost of cyber crime**

Loss of Trade Secrets

$749B or more lost annually as cybercriminals steal intellectual property*

Cost of protection

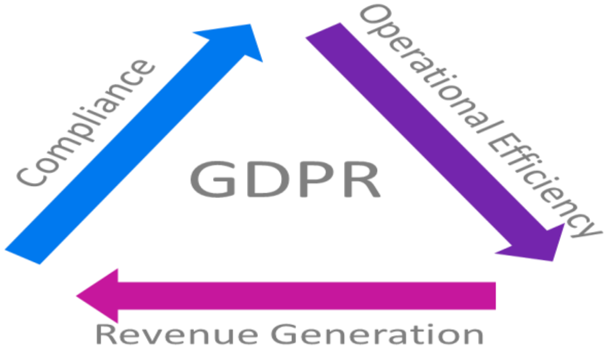
3.8% of total IT budget spent on security, reduction from 4% in 2014*

Reactive vs. proactive

56% of executives say their response to security is reactive, not proactive***

Key Points

- Security is a board of directors concern
- Security leadership is under immense pressure
- Need for greater visibility of **business risks** and to make sound security investment choices



Sources: *PWC global state of information security survey report 2015; **Ponemon 2015 Cost of cyber crime study: Global; ***Ponemon 2014 report on senior executive response to security

Managing risk in today's digital enterprise

Enterprise IT
will continue to transform

The adversary
is innovating

The assumption of compromise

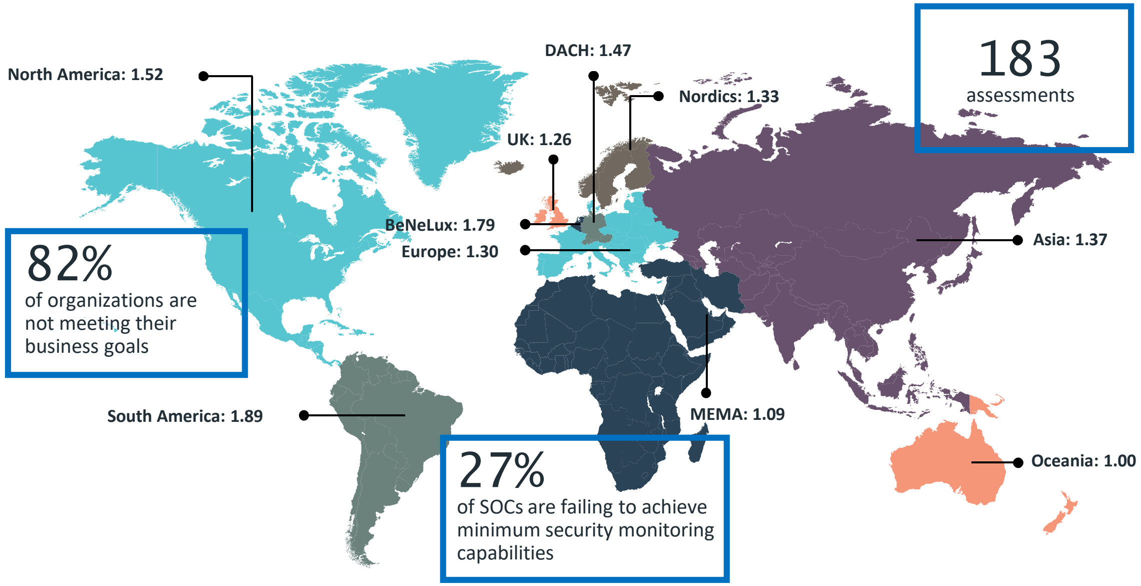
Regulations
Complexity & costs are rising

Skills
Scarcity is a top challenge

Doing the simple stuff is hard

2017 State of Security Operations

4th annual report



183 assessments

82% of organizations are not meeting their business goals

27% of SOCs are failing to achieve minimum security monitoring capabilities

Top observations

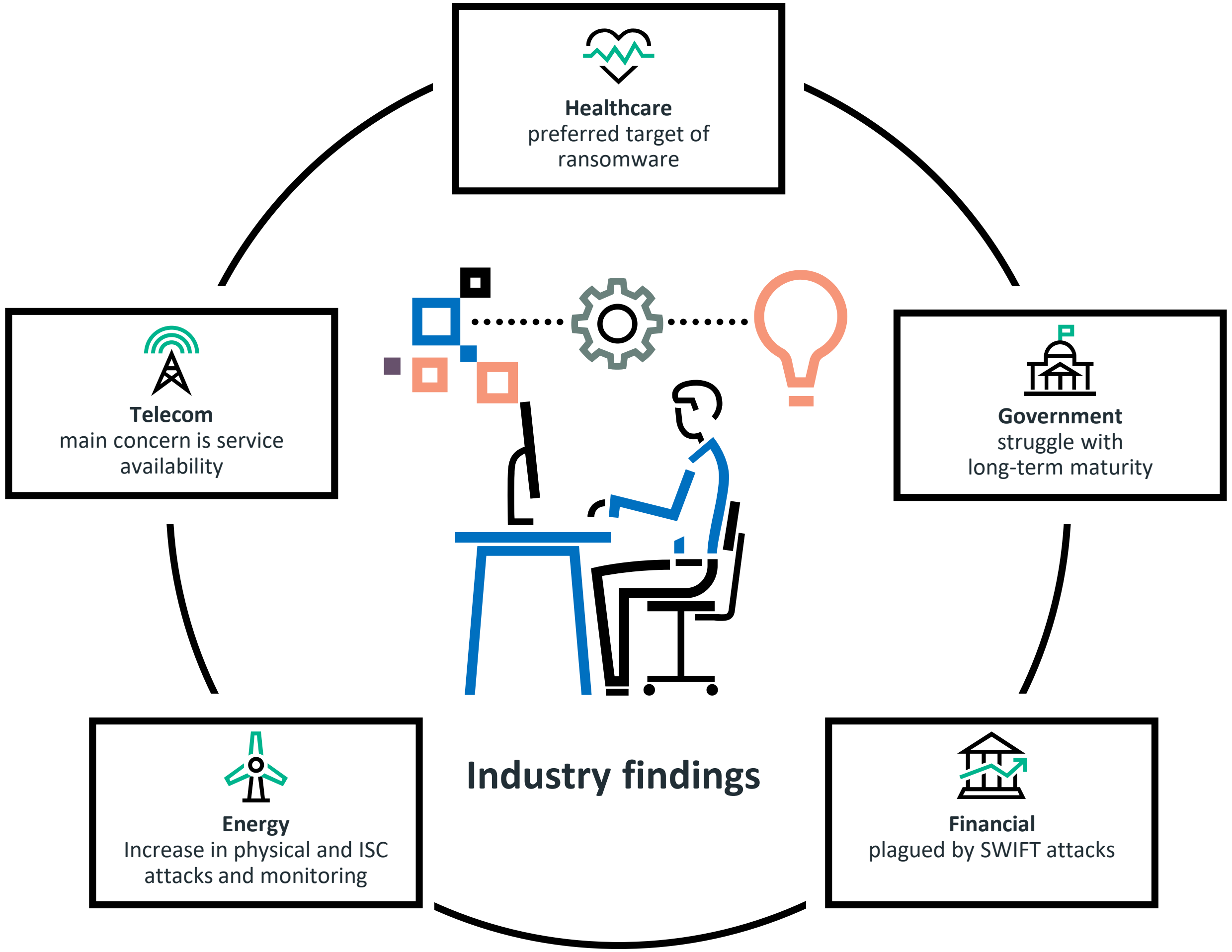
Full automation of operations is unrealistic

Hunt-only search & response does not provide full coverage and effectiveness

Increased capabilities come from **hybrid staffing** solutions

Continuing trend
Proliferation of threat hunt programs

Emerging trend
Development of security fusion centers



Industry findings

Healthcare
preferred target of ransomware

Telecom
main concern is service availability

Government
struggle with long-term maturity

Energy
Increase in physical and ISC attacks and monitoring

Financial
plagued by SWIFT attacks

Read the full report at

https://software.microfocus.com/en-us/asset/2017-state-security-operations

Top 3 findings:

- Full automation of operations is unrealistic
- Hunt-only/search approaches do not provide full coverage and effectiveness
- Increased capabilities come from hybrid staffing

Findings

Decreased maturity with hunt-only programs – Success is had when hunt is additive to stable real-time detection and response. Immaturity comes from hunt and search non-repeatable approaches.

Development of Fusion Centers – Getting real value out of your cyber threat intel. Leveraging the maturity of individual BUs across the org.

Providing Effective business metrics – Focus on reporting things that matter to the business (not # of infected machines, etc.)

Findings Continued

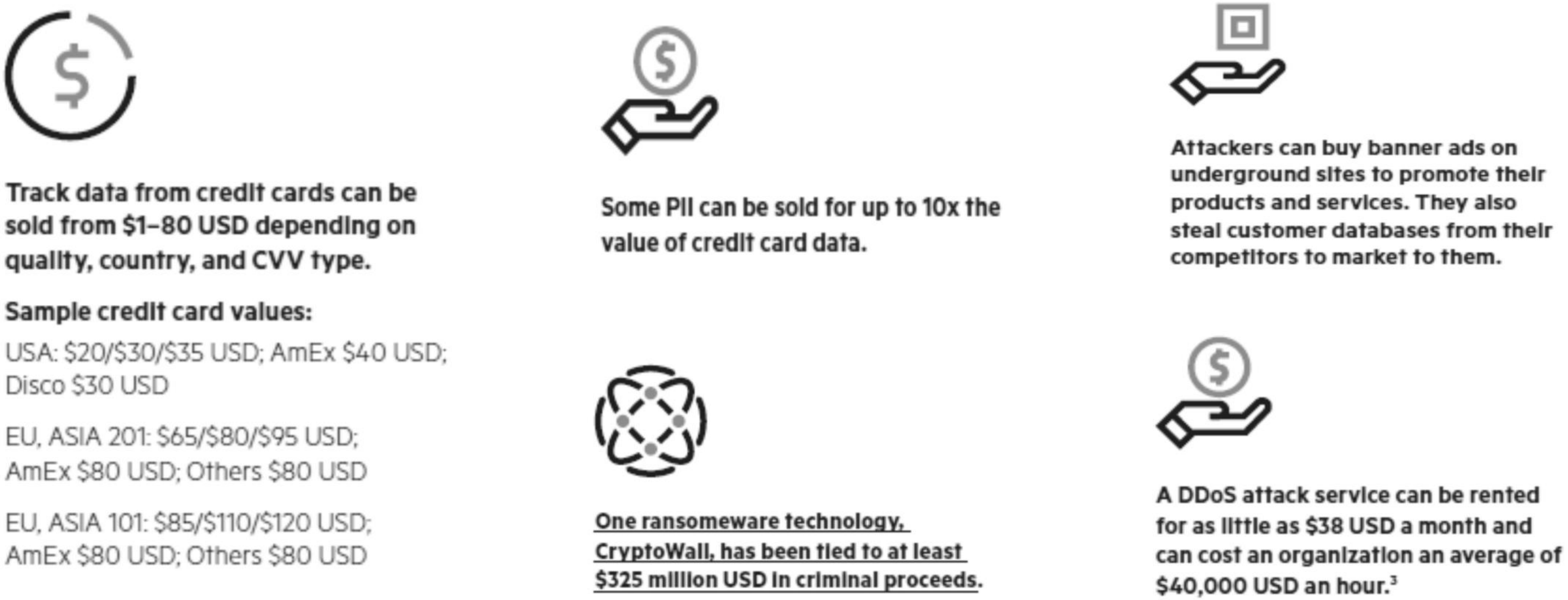
Commercial vs. Open source tools in security operations – Focus on security vs. focus on maintaining tools.

Automation and Elimination of entry level analysts – Full automation is not realistic. Advanced threats require human investigation. Risk assessments still involve human reasoning.

Organization size: There is no link between size of organization and maturity. Maturity more tied to goals of security organization.

The use of security as competitive differentiator, market leadership and industry alignment = predictors of maturity.

To Manage Risk - Understand the Business of hacking ?



Track data from credit cards can be sold from $1–80 USD depending on quality, country, and CVV type.

Sample credit card values:

USA: $20/$30/$35 USD; AmEx $40 USD; Disco $30 USD

EU, ASIA 201: $65/$80/$95 USD; AmEx $80 USD; Others $80 USD

EU, ASIA 101: $85/$110/$120 USD; AmEx $80 USD; Others $80 USD

Some PII can be sold for up to 10x the value of credit card data.

One ransomeware technology, CryptoWall, has been tied to at least $325 million USD in criminal proceeds.

Attackers can buy banner ads on underground sites to promote their products and services. They also steal customer databases from their competitors to market to them.

A DDoS attack service can be rented for as little as $38 USD a month and can cost an organization an average of $40,000 USD an hour.[3]

The Business of Hacking is a very lucrative business for the Adversaries

To Manage Risk - Understand The business of hacking ?

To understand the business of hacking we must understand every step in the value chain of the underground economy. Only then can we work to disrupt it.

Human Resources – Operations – Logistics – Marketing & Sales – Research & Development

99+

2017 - 99 days
2016 - 146 days
2015 - 229 days

Mandiant M- Trends Report 2017

Average time bad guys are inside **before detection**

2015 ...March April May June July August September October November December **2016** January February March…

of breaches occur at the **application layer** **84%**

2. http://www.neowin.net/news/hp-discover-startling-security-statistics and HPE Research

70 days

Average Remediation Insider Threats

Ponemon Cost of Cyber Crime Report

59% of breaches are reported by a **3rd party**

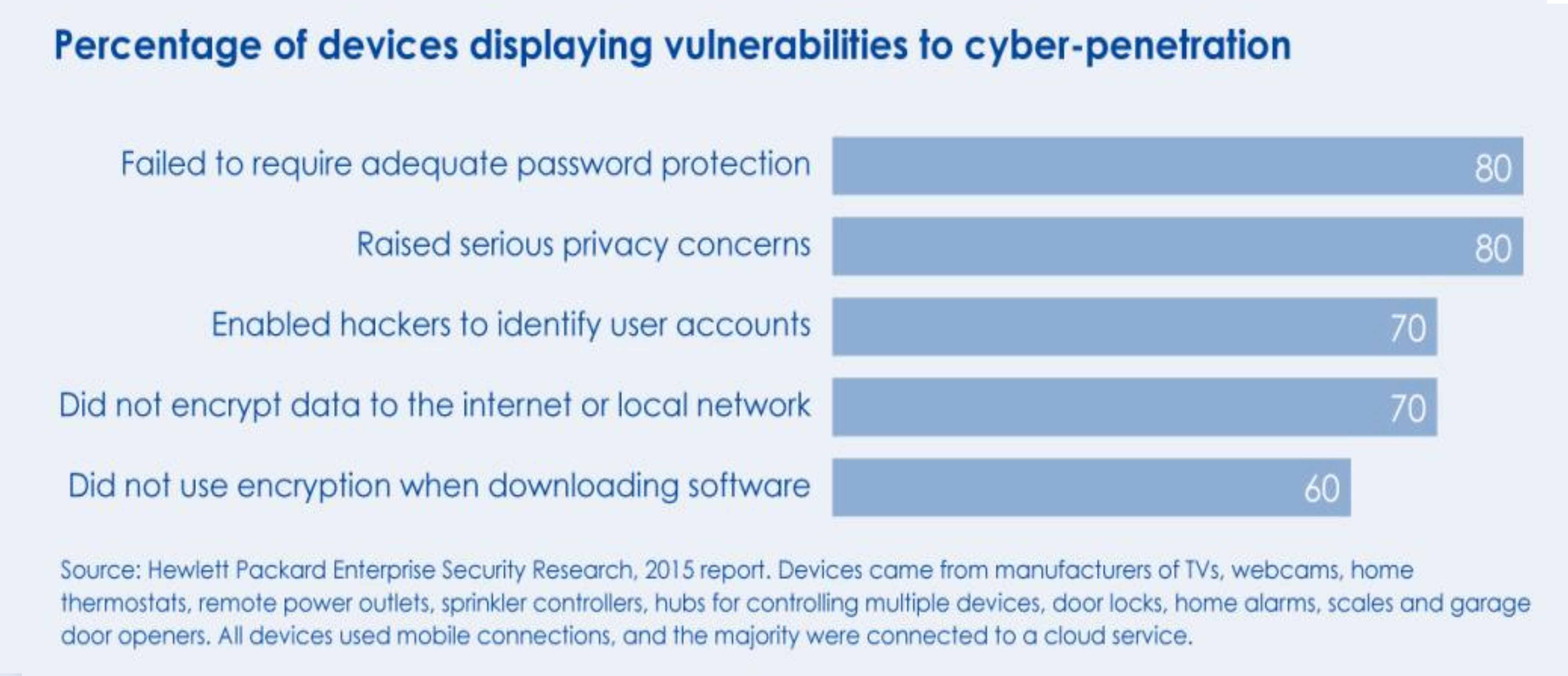
Trustware 2016 Global Security Report

23% ROI **Security Intelligence**

21% ROI **Encryption Technology**

Ponemon Cost of Cyber Crime Report

The evolving landscape



Percentage of devices displaying vulnerabilities to cyber-penetration

Source: Hewlett Packard Enterprise Security Research, 2015 report. Devices came from manufacturers of TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers. All devices used mobile connections, and the majority were connected to a cloud service.

28.1 billion connected things by 2020 according to IDC

In 2016, 5.5 million new “things” will get connected every day - Gartner

“2017 will be the year of the Data Bandit”

2014 was the year **of Point-of-sale** (POS) targeted malware attacks
2015 was the year of the **Healthcare / Medical** attacks
2016 is becoming the year of the **Critical National Infrastructure, Education** & **IoT** attacks

Seven Recommendations for immediate action by CIOs & CISO’s

1. Adopt a **comprehensive framework** and strategy for digital security
2. Focus on the **DATA** - **records management**, **classification**, **encryption** and **retention**
3. Conduct a **full audit** of current and **likely risks initiatives**
4. Bake **security into all processes** (Security by design)
5. Mobilize the larger workforce around **data security** (product design, supply chain …)
6. Bring **partners** & **customers** up to rigorous security standards
7. Rethink the role of IT (become a **valued business partner**)

KEEP CALM

AND

PREPARE

FOR THE

GDPR

MICRO FOCUS®

Kiitos / Thank you

Tim Grieveson
Chief Cyber & Security Strategist

www.gdprandbeyond.com

✉ tim.grieveson@microfocus.com

in https://uk.linkedin.com/in/timgrieveson

@timgrieveson

#DataBandit @timgrieveson @MicroFocusSec