Phoenix 2.0

IT Without the Drama

The Middle Market & Cyber Security

Outline

The Definitions

2017 Year in Review

Business Implications

Threat Actors

Attacks

What Should We Do?

Helpful Definitions

The Definitions

Cybersecurity is the protection of information & systems from attack, damage, and unauthorized access.

Incidents *vs.* Breaches

We talk a lot about incidents and breaches and we use the following definitions:

Incident—a security event that compromises the integrity, confidentiality or availability of an information asset.

Breach—an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

What is Middle Market?

We work mostly in lower middle market <100m —mostly unregulated industries.

33%

Of the US private sector GDP

60%

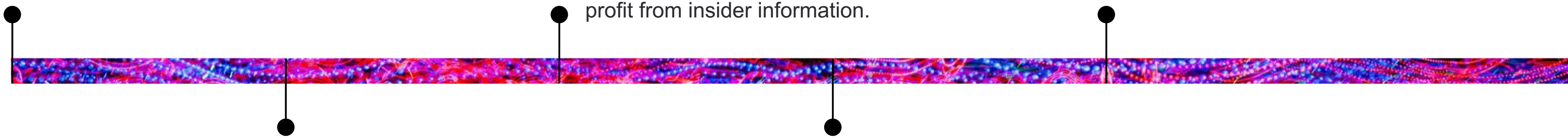
Of all new jobs created

$10M–1B

Revenue

ANATOMY OF AN ATTACK

2017 Year in Review



Equifax

Unpatched Apache Struts web servers

DeLoitte

Stolen corporate email creds from IT guy

SEC—EDGAR DB system breach

DB holds documents publicly traded companies have to file with the regulator may have allowed hackers to profit from insider information.

DLA Piper—RansomWare

“One of the world’s biggest law firms, is still struggling with the effects of last week’s global cyber attack, with employees’ access to emails and documents severely curtailed in what insiders have called a “disaster”

WannaCry, Not Petya (RansomWare): Maersk, Merck, FedEx

1B in damages and lost revenue

Business Implications of Bad Security Posture

If you don't understand what happened (breach/incident), how can you assess the impact or know which laws to abide by? There are 48 different statues + Guam & D.C. = a confusing legal web of state breach notification laws, with no overarching federal framework

01 | Bad for M&A

02 | Sink a business and management careers

03 | Extortion, serious business disruption, IP/data loss, litigation

NetDiligence/McGladrey's 2016 Annual Cyber Claims Study

Middle market companies—those with revenues between $50M and $1B—account for nearly half of all cyber claims. *only 22% have cyber coverage

NCMM's Cyber Security and the Middle Market Report

Companies that rated cybersecurity as "*extremely important*" saw revenue growth of **7.8%**, while those that deemed it "*very important*" saw revenue growth of **4.7%** and those who rated it "*not important*" saw growth of **3.9%**.

The average breach costs approx. **$4M**, per the Ponemon Institute, so it isn't surprising to see companies saving money even when spending on cybersecurity.

Deloitte Report—Technological immaturity in the middle market

56% of middle market companies were in the deployment phase of cloud computing in 2016, up from **26%** in 2013.

Approximately **29%** of midmarket companies had a successful, mature deployment of a cloud solution in 2017, up from **21%** in 2015.

61%

Of data breach victims are businesses with less than 1,000 employees

Verizon Data Breach Report

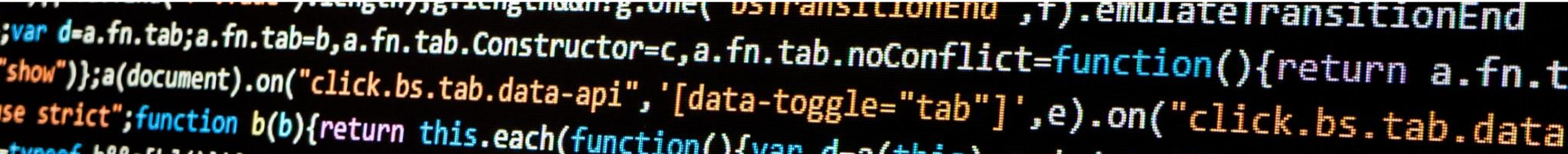
Middle Market companies are targets for supply chain attacks

Entry-Way Into Large Enterprises

Lots of data and money, not a lot of maturity or security, delay in finding out if breached and then just sweep it under the rug.

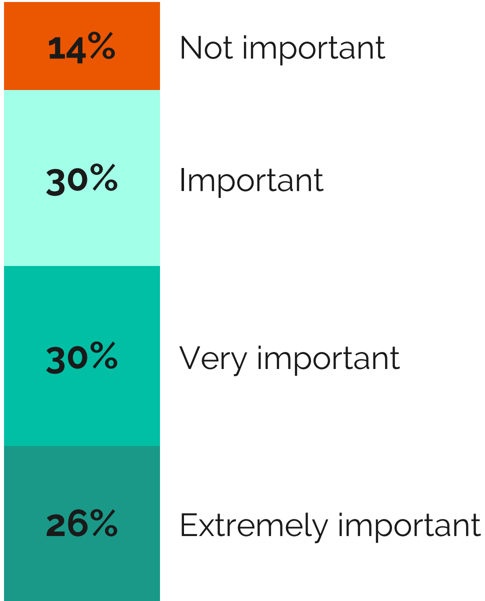
Back in *July 2017*, up to **14M** U.S.-based **Verizon** customers had their data exposed by a third-party partner, which misconfigured a repository storing the personal information it had access to

Last month misconfigured **Amazon S3** Simple Storage Service bucket, managed by a **Walmart** jewelry partner, left personal details and contact information of **1.3M** customers exposed to the public internet.

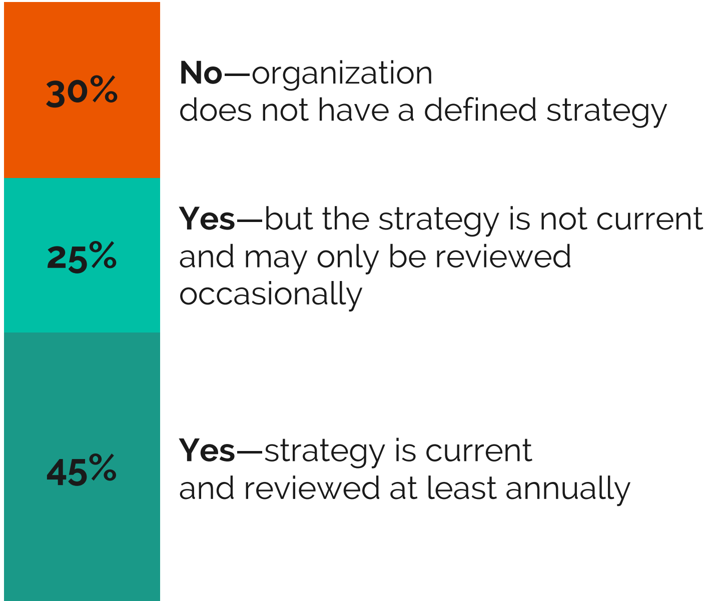


```
g.one("bsTransitionEnd",f).emulateTransitionEnd
;var d=a.fn.tab;a.fn.tab=b,a.fn.tab.Constructor=c,a.fn.tab.noConflict=function(){return a.fn.t
"show")};a(document).on("click.bs.tab.data-api",'[data-toggle="tab"]',e).on("click.bs.tab.data
se strict";function b(b){return this.each(function(){var d=a(this)
```

Importance of Cybersecurity



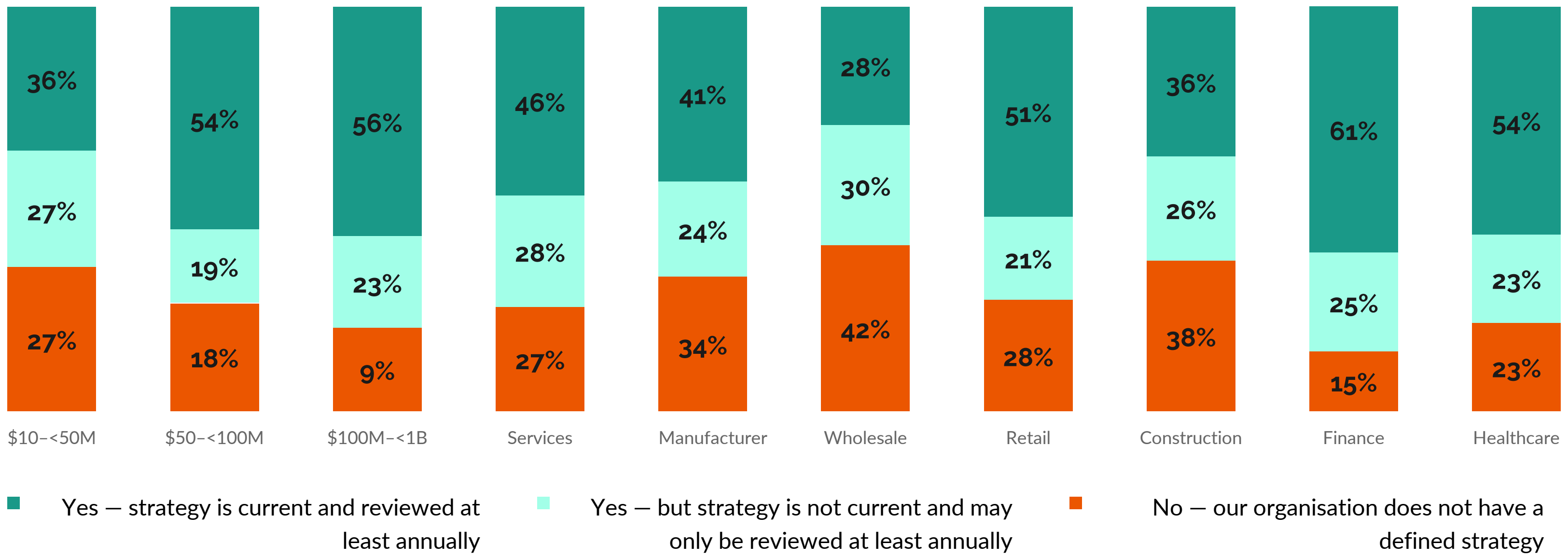
Cyber Risk Strategy Defined



The Strategy

Bigger companies and certain industries are more likely to have a defined cybersecurity strategy.

Whether organization has defined cyber risk strategy



Hard to find breach & other data as privately owned and not regulated = don’t need to disclose

1. No overarching body that tracks breach or incident data

2. No incentive to report

3. No incentive to do root-cause analysis

4. Most cyber policies don't cover root cause analysis

The Facts

Mid-sized and smaller companies are at a disadvantage for hiring information security staff. 100K new U.S. engineering graduates per year, only about 3K have security credentials, and those high-priced individuals are snapped up by larger organizations.

Verizon DBIR: Studied 70 Incidents detected by mid-size companies in the past year have led to an estimated financial lost of $1.8M per company.

Not only could the client companies end the business relationship, they might also hold the services provider legally responsible for their damages and damages to their customers.

Most breaches at mid-size businesses aren’t as large as the ones that make national headlines: on average from 1K to under 100K people affected.

Types of Attacks

1. **Insider and privilege misuse**—trusted actors leveraging logical and/or physical access in an inappropriate or malicious manner.
2. **Cyber-espionage**—targeted attacks from external actors hunting for sensitive internal data & trade secrets.
3. **Web application attacks**—web-app related - stolen credentials or vulnerability exploits.
4. **Crimeware**—malware incidents, typically opportunistic and financially motivated in nature (e.g., banking Trojans, ransomware).
5. **POS Intrusions**—attacks on POS (Point-of-sale) environments leading to payment card data disclosure. Payment card skimmers—physical tampering of ATMs and fuel-pump terminals.
6. **Denial of service (DoS) Attacks**—non-breach related attacks affecting business operations.
7. **Physical theft & loss**—physical loss or theft of data/IP or IT-related assets.

Attack Vectors

1. **The Human Element**—scenarios involving human-related threat actors or targeted victims.
2. **Conduit Devices**—scenarios involving device misuse or tampering.
3. **Configuration Exploitation**—scenarios focusing on reconfigured or misconfigured settings
4. **Malicious Software**—four scenarios centering on sophisticated or special-purpose illicit software

The Human Element	HE-1	**Financial Pretexting**
	HE-2	**Hactivist Attack**
	HE-3	**Partner Misuse**
	HE-4	**Disgruntled Employee**
Conduit Devices	CD-1	**C2 Takeover**
	CD-2	**Mobile Assault**
	CD-3	**IoT Calamity**
	CD-4	**USB Infection**
Configuration Exploitation	CE-1	**Website Defacement**
	CE-2	**DDoS Attack**
	CE-3	**ICS Onslaught**
	CE-4	**Cloud Storming**
Malicious Software	MS-1	**Crypto Malware**
	MS-1	**Sophisticated Malware**
	MS-1	**RAM Scraping**
	MS-1	**Unknown Unknowns**

The Actors

The Actors

International state sponsored

Chafer group — hitting major telecom companies in the Middle East and attack on a major international travel reservations firm, targeting Saudi Arabia most recently.

North Korea

Hidden Cobra/Lazarus Group: 2014 attack on Sony Pictures, stole $12M from Banco del Austro Ecuador, attack on the Bangladesh Bank, successfully stealing $81M through SWIFT terminal compromise.

Fancy Bear APT

Thought to be responsible for attacks on: German parliament, French television, White House, NATO, DNC and Emmanuel Macron.

The Actors

Organized crime

Carbanak—Ukrainian crime gang. Baking malware that stole up to $1B. *Cebola Chan 3.0* — spanish language darkweb forum, busted in 2016

Legit companies that make exploits and sell them legally

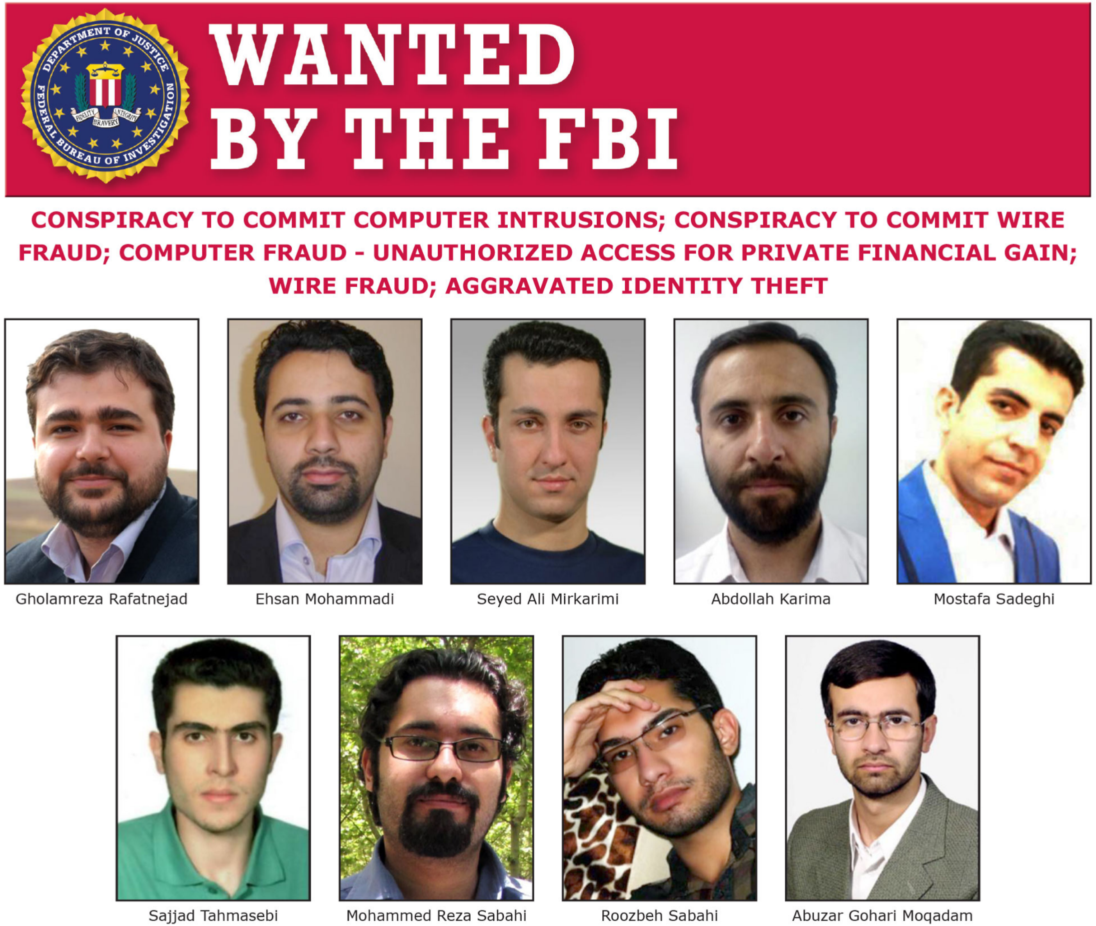
NSO Group (Israeli) created spyware used to compromise UAE activist's iPhone. It was sold to an Arab company with permission from Israeli Defense Ministry.

Cryptomining gangs

Group One, cryptogang commanded a botnet of 10k machines, consumer to corporate PCs and servers that were stretched across the globe to mine Monero

Threat Actors

without hoodies 😉



WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER INTRUSIONS; CONSPIRACY TO COMMIT WIRE FRAUD; COMPUTER FRAUD - UNAUTHORIZED ACCESS FOR PRIVATE FINANCIAL GAIN; WIRE FRAUD; AGGRAVATED IDENTITY THEFT

Gholamreza Rafatnejad

Ehsan Mohammadi

Seyed Ali Mirkarimi

Abdollah Karima

Mostafa Sadeghi

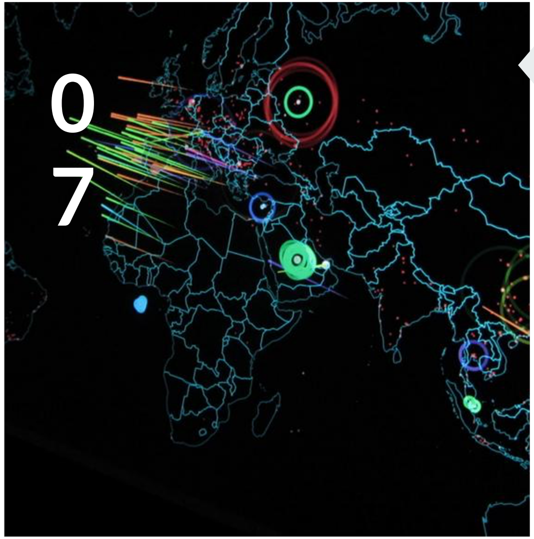
Sajjad Tahmasebi

Mohammed Reza Sabahi

Roozbeh Sabahi

Abuzar Gohari Moqadam

The Actors



07

Hacktivists, political/privacy advocacy groups

EFF defends individuals and new tech. from legal threats, gov. malfeasance, provide guidance to the gov. & courts, organizes political action, supports technologies that preserve personal freedoms & online civil liberties, challenges legislation which infringes on liberties & fair use, fights against abusive patents. ***Anonymous*** is a decentralized hacktivist group that is known for DDOS cyber attacks against gov. Institutions, corporations, Church of Scientology.

08

The good guys

Google's Project Zero is the name of a team of security analysts employed by Google tasked with finding zero-day vulnerabilities. It was announced in July 2014. Cisco Telos group, corporate Red teams/Blue teams

Incident Examples

1. Retail

An online retailer had noticed unusual activity on its server, which prompted an investigation. They discovered that hackers had stolen an employee’s credentials and used them to access the names, billing addresses and credit card numbers of approximately **50,000 customers** during checkout.

Outcome

The organization retained the appropriate vendors and notified the necessary individuals and agencies.

The retailer incurred approx. **$1M** in first-party costs.

2. Healthcare

A hospital office employee had stolen medical profiles, histories and detailed personal information on approximately **125,000 patients**.

Outcome

Insurance company provided the hospital with crisis support team, made up of outside vendors, to help resolve the breach and reimbursed the hospital approx. **$800,000** for the crisis team’s expenses.

3. Technology Professional Services

A service provider of application security services contracted with a social welfare organization to update the security of its legacy IT systems.

The social welfare organization filed suit against provider after a security incident, claiming it failed to meet contractual obligations, delivered a poorly architected system and failed to properly inform client of risks

Outcome

The social welfare organization sought damages in excess of **$15M**.

4. Manufacturing

A consumer products company had undergone a software system upgrade performed by a vendor to patch an insecure legacy application

The system upgrade failed, which caused all of the manufacturer’s systems to malfunction on the same day.

This caused an unintentional/unplanned outage, which resulted in the suspension of the manufacturer’s operations.

Outcome

$2M was paid out for expenses associated with the business interruption.

What Should Middle Market Companies Do?

1. Have a relationship with a forensic security firm
2. Have a relationship with a law firm that specializes in cyber and data privacy (e.g. JMBM)
3. Have cyber insurance
4. Invest in DLP and or SIEM because loss or exfil triggers breach notification laws and potential litigation

Takeaways

Today the most widely talked about topic in middle market & small company security is about them being a supply chain threat vector to their larger customers, vendors and partners.

1. Cyber security is not just a business issue, it’s a societal one, as trusted advisors, it's your resp. to warn them
2. Are you secure?
3. What if you’re the gateway for an attack on your client?

Questions?

Sources

- 🔗 Cybersecurity and the Middle Market
- 🔗 Middle Market Growth
- 🔗 Verizon 2018 Data Breach Investigations Report
- 🔗 Mergers & Acquisitions
- 🔗 The Middle Market Monthly
- 🔗 Middle Market Executive
- 🔗 Understanding Cyber Insurance Risks of Target Companies
- 🔗 Deloitte Middle Market Technology Trends Report

Thank you!

alex@p20inc.com (415) 595-2703
90 S. Spruce, Suite C-1, South SF, CA 94080

p20Inc.com