

The Cyber War on Small Business

Dillon Behr
Executive Lines Broker
Risk Placement Services, Inc.



Meet Our Speaker



Dillon Behr Executive Lines Broker Risk Placement Services, Inc.

- Previously worked as Cyber Security threat Intelligence Analyst for Discover Financial Services and the US government.
- Focused on finding cyber liability and breach response solutions for clients of all types and sizes.
- Risk Placement Services (RPS) is a Managing General Agent/Underwriting Manager and nationally focused wholesale insurance broker.
 - Ranked in the top five in every insurance industry category and have been consistently ranked as the largest MGA in the country for several years.
 - Known for doing the right thing even if it means referring business to a competitor



The Cyberwar on Small Business

According to the 2016 State of SMB Cybersecurity Report, in the last 12 months, hackers have breached **HALF** of all small businesses in the United States



Small Business Are:

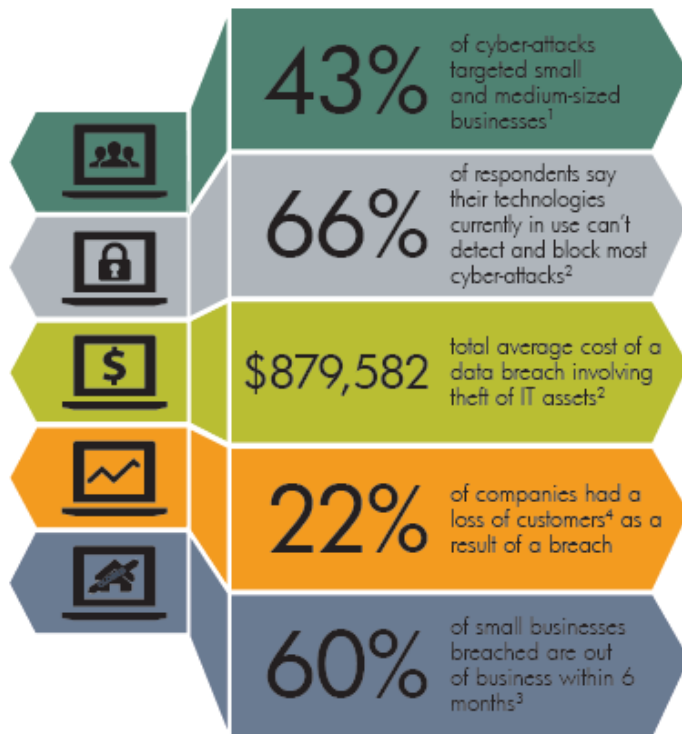
- the **principal targets** of cyber crime
- **especially susceptible to phishing attacks via email** or fraudulent activity happening in their e-commerce shops.

Attacks can **derail money-making activities** for up to a week

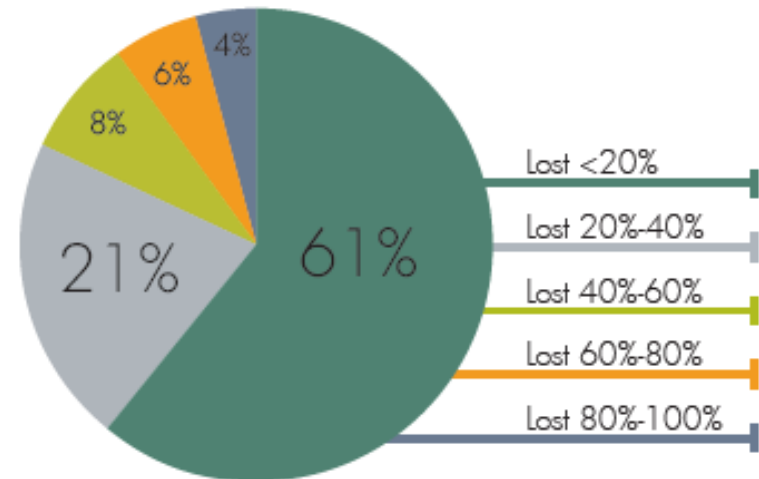


The Stats

Know The Facts



Percentage Of Customers Lost By Companies Due To Attacks⁴



1. Source: Symantec
2. Source: The 2016 State of SMB Cybersecurity - Ponemon Institute and Keeper Security
3. Source: National Cyber Security Alliance
4. Source: Cisco 2017 Security Capabilities Benchmark Study, www.cisco.com/go/acr2017

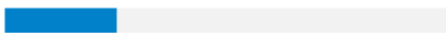


Who's Behind Breaches?



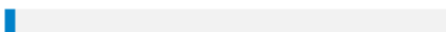
Who's behind the breaches?

75% 
perpetrated by outsiders.

25% 
involved internal actors.

18% 
conducted by state-affiliated actors.

3% 
featured multiple parties.

2% 
involved partners.

51% 
involved organized criminal groups.



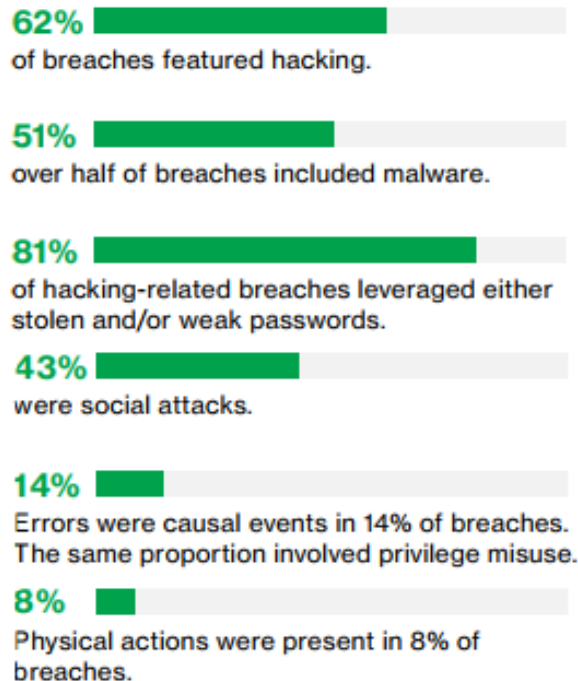
* Verizon 2017 Data Breach Investigations Report



What Tactics are Used?



What tactics do they use?



- Hacking
- Malware
- Stolen/weak passwords
- Social attacks
- Errors/Privilege misuse
- Physical actions

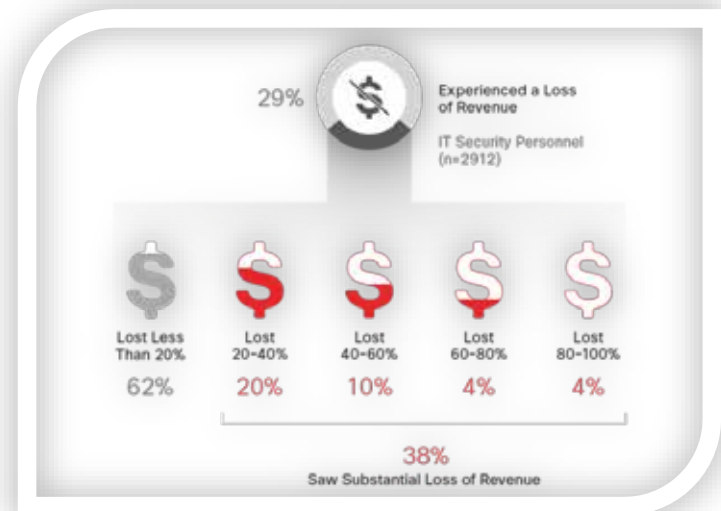
* Verizon 2017 Data Breach Investigations Report



Effects of Cyber Breaches



% of Business Opportunity Lost



% of Organizational Revenue Lost



Business Functions Most Likely to be Effected



Small Businesses Should Focus on Cyber Security

- Most business, regardless of size, collect, process, and store large amounts of data on computers and other device
- This data could be sensitive information for which unauthorized access or exposure could result in negative consequences if breached
- When this data is transmitted from one device to another while doing business, it is important that this data is protected from cyber attacks



A Cyber Attack is Inevitable

Does your business have technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access?



RESPOND, RESTORE, ENSURE

The National Cyber Security Alliance advises that companies must be prepared to “**RESPOND** to the inevitable cyber incident, **RESTORE** normal operations, and **ENSURE** that company assets and the company’s reputation are protected.



Being PROACTIVE is the 1st Step

- Perform software updates - #1 overlooked thing that small business owners don't do
- Enable two-factor authentication
- Perform regular backups of company data
- Create stronger passwords
- Install antivirus software
- Purchase Cyber Liability Insurance – helps to mitigate losses from a variety of cyber incidents, including data breaches, business interruptions and network damage.



Data Breaches Can Occur Offline Too

- A cyber breach is not the only way that business data can be compromised.
 - Physical theft can also result in data breaches when your company data (computer, server, mobile device, or physical records) is taken without authorization.

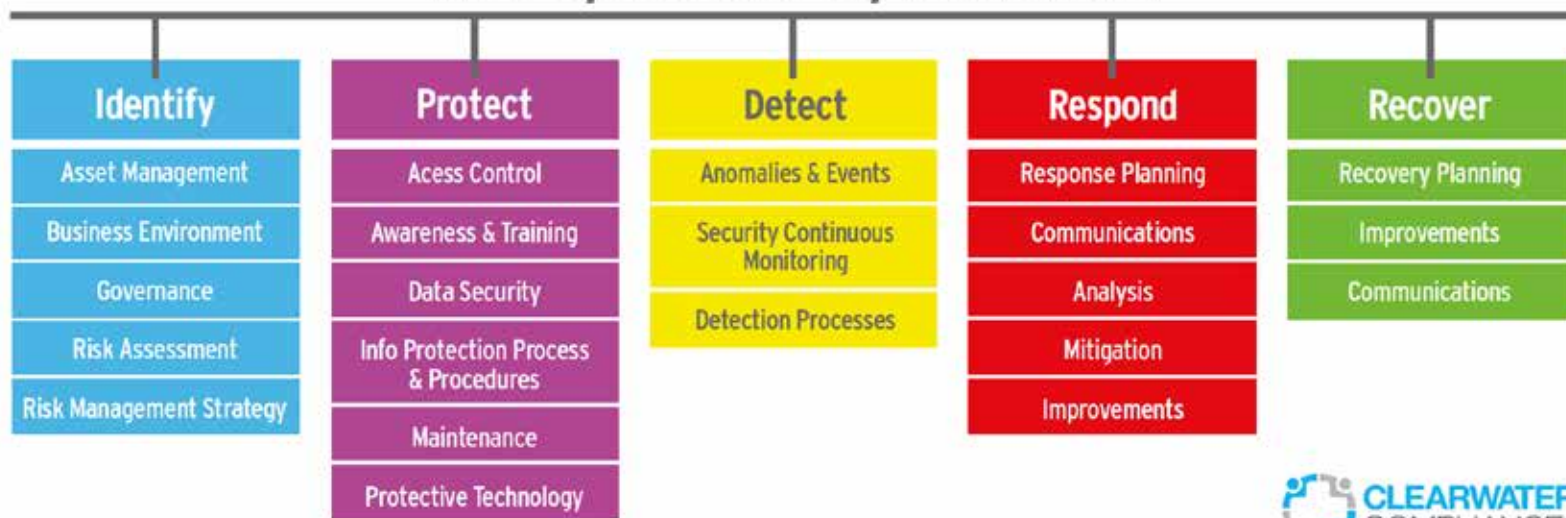
Treat physical security with the same level of attention as cyber security.

Monitor and restrict access to stored data, enforce strict policies regarding locking and protecting computers and mobile devices, establish strict policies for data disposal, and train employees to be aware of suspicious activities.



Data Handling Best Practices & Guidelines

NIST Cyber Security Framework

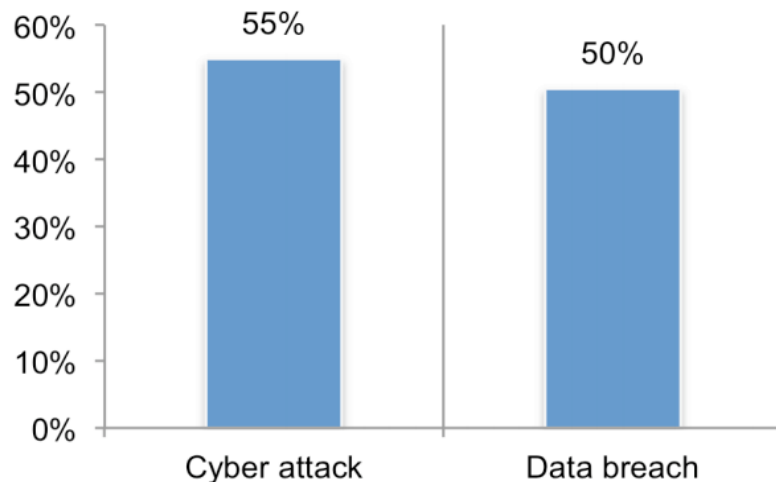


Attacks Will Cost You!

- 82% of small business owners don't think they will be attacked because they don't have anything worth stealing. This is why they are targeted by hackers!

Figure 1. Our organization experienced a cyber attack and data breach in the past 12 months

Yes responses



Cyber Security Statistics – Numbers Small Businesses Need to Know (www.smallbiztrends.com)

- These companies spent an average of **\$879,582** because of damage or theft of IT assets
- Disruption to normal operations cost an average of **\$955,429**
- Emails, phone numbers and billing addresses are valuable to cyber criminals
- NFIB can help your business access protection through NFIB Commercial Insurance.



QUESTIONS?

