The anatomy of a DATA BREACH

SIZE DOESN’T MATTER

Many organizations feel they have nothing worth stealing. That they are too small and invisible. However, with the rise in breaches, any data has value to your hackers, and your information is at risk.

YOUR DATA HAS VALUE TO AN ATTACKER

40M records X $2/record = $80M in attacker profit
NO ONE IS SAFE
Small and midsized businesses are vulnerable for credit card data, personal information and employee records theft due to weak security measures.

Attacks on businesses
- 94% of businesses under 1,000 employees
- 6% of businesses over 1,000 employees

ALL INDUSTRIES ARE VULNERABLE
Companies in all industries are at risk for an attack.

Affected areas
- 24% financial organizations
- 15% consumer products
- 12% manufacturing warehouse distribution
- 31% information and professional services
- 18% other
THE DAMAGE DONE

The cost of a breach is significant, both financially and reputationally.

Average amount spent per year to resolve incident

$10M

No cap on damages

Hackers will find vulnerabilities

Data theft has become big business and if you have issues with your security, chances are they will be exploited.

Think you’re protected? Unprotected emerging technologies

76% accessed weak or stolen credentials

49% of businesses not securing employee mobile devices

The threat is rising

Some organizations feel they have nothing worth stealing. They are too small and invisible. However, with the rise in breaches, any data has value to your hackers, and your information is at risk.
The attacker

WHAT’S THE MOTIVATION?

Intellectual property theft + VPN access to pose as others + Email access to send spam =

YOU MAY KNOW THE ATTACKER, BUT YOU PROBABLY DON’T

Many assume that attacks come from inside the organization, but that is not necessarily true.
When the victim and attacker meet

**HOW DOES THIS HAPPEN?**

We are all in the same data-driven ecosystem, and access points are more numerous than you may think.

More breaches come from simple attacks such as malware, skimming and phishing than from targeted criminal efforts.

- **78%** rated as low difficulty
- **75%** opportunistic attacks
- **71%** targeted user devices

If you do not have the proper measures in place, discovering criminal activity is difficult, even after it has taken place.

- **82%** discovered by third party
- **75%** took weeks to discover
- **60%** of small and midsized businesses out of business within six months

No cap on damages
Vulnerability is driven by your need to collect, analyze and share data. Those needs will only grow in the future, and information will become more valuable to criminals, increasing your exposure to attacks. Are you aware of your points of vulnerability?

- Have you taken the right steps toward effectively mitigating risk?
- Are you in line with regulatory and legal security and privacy requirements?
- Do you have current policies and procedures based on your organization’s current risk exposure?

Learn more about McGladrey’s security and privacy Rapid Assessment®, and how it can help protect your organization against the significant financial, reputational and compliance damage just one data breach can cause.