Cyber attacks on small businesses are a common occurrence. While smaller organizations often lull themselves into thinking cybercriminals aren't interested in them, reality is quite different. It's true the biggest headline-grabbing hacks typically involve large companies, but anyone could be a target. Hackers don't discriminate by size.

Take a look at these six headlines from 2019:

- "Business Forced to Close"
- "Compromised POS Systems"
- "23K+ Patients Compromised"
- "Don't Become a Headline"
- "All Files Deleted"
- "75K Ransom Paid"

"Customer Information Exposed"
Story 1

In January, cyber thieves ran roughly 100,000 stolen card numbers through the payment system of Innovative Higher Ed Consulting Inc., resulting in a $27,000 payment to reverse the charges. By May, Innovative Higher Ed Consulting was closed due to the attacks.
83% of SMBs lack the funds to deal with the repercussions of a cyber attack.

Source: https://www.insurancebee.com/blog/smb-owners-unprepared-for-cybercrime
In February, Connecticut-based optometrists Dr. Thomas DeLuca, Dr. Anthony Marciano & Associates notified about 23,578 Patients that their personal data was potentially breached during a ransomware attack.
58% of SMBs who experienced a cyber attack in the past 12 months, reported loss or theft of sensitive information about customers or employees.

Source: Ponemon Institute's 'The 2018 State of Cybersecurity in Small and Medium Size Businesses'
In February, local Minnesota restaurants had their customer's credit card information stolen after malware was deployed to their POS systems. Stolen information potentially included the cardholder's name, credit card number, expiration date, and CVV.
Overall web attacks on endpoints - like a POS system - increased by 56% in 2018.

Source: Symantec's Internet Security Threat Report February 2019
In April, after refusing to pay a ransom to their hackers, Michigan-based Brookside ENT and Hearing Center was forced to close when hackers deleted all patient files during a ransomware attack.
The SMBs who experienced a cyber attack in the past 12 months lost an average of 10,848 individual records.

Source: Ponemon Institute's 'The 2018 State of Cybersecurity in Small and Medium Size Businesses'
In June, NEO Urology in Boardman, Ohio was infected by a ransomware attack, which hacked its entire IT system and left all of its data encrypted, until they paid a ransom of $75,000.
Cyber attacks are expensive for SMBs, with the average cost of a single incident running

$53,987

Source: Continuum's 'Underserved and Unprepared: The State of SMB Cybersecurity in 2019'
In July, a Lincoln-based insurance and financial company had several of its employees fall victim to phishing scams which tricked them into providing their email credentials. As a result, they may have exposed customer's names, addresses, and Social Security numbers.
76% of businesses reported being a victim of a phishing attack in 2018.

Source: ProofPoint’s ‘2019 State of the Phish Report’
Comcast Business SecurityEdge™ can help deter some cyberthreats.

For more information visit, comcastbusiness.com/SecurityEdge