



Cybersecurity

What Every Business Needs to Know

Are you protected from potential network and privacy exposures? Any business that uses technology to collect confidential customer information needs to know the facts – and risks – associated with data breach liability and not having proper network security, privacy and cyber protection.

The high cost of data breach



\$3.86M

Average cost of data breach paid by U.S. companies¹

Widespread risk



27% of data breaches in 2017 were due to employee or owner accidental release of private data.¹



Small business cyber attacks increased from 61% in 2017 to 67% in 2018.²



The three most frequently breached sectors are Health Care (18%), Professional Services (18%) and Retail (11%).³



Hacking is the highest cause of data loss (27%), followed by Malware/Virus (18%). Insider involvement was reported in 38% of the incidents.³



Companies with less than \$50M in revenue were the most impacted, accounting for 47% of the claims.¹



Lost or stolen device claims more than doubled and paper records claims almost tripled last year.¹

Data breach by the numbers

3.6B

records exposed⁴

3,676

reported breach incidents through first nine months of 2018⁴

Cost per compromised customer record¹



Health Care
\$409



Services
\$181



Industrial
\$152



Financial
\$206



Education
\$166



Technology
\$170

4 REASONS

Why you need Cyber Liability/Security protection in 2019

- 1 Stringent laws/regulations
- 2 Advances in technology
- 3 Global outsourcing
- 4 User error

¹ 2018 Cost of a Data Breach Study sponsored by IBM Security with research independently conducted by Ponemon Institute LLC, ² Ponemon Institute, LLC - "2017 State of Cybersecurity in SMBs," ³ NetDiligence* 2017 - Study of Cyber Claims, ⁴ Risk Based Security 2018 Q3 Data Breach Quick View Report