Resource planning for Executives:

07

Reasons to Increase Your Cybersecurity Budget

01

The overall cost of cybersecurity has increased

Sped up dramatically by the Covid-19 pandemic, remote work is now here to stay. This is one reason cybersecurity costs more now than ever. More remote workers means more access points for hackers.

- Web and email security will grow 12.5% in 2021
- Identity access management, underpinning secure access to data and applications, will grow 10.4%
- Network security will increase 8%

02

Training costs for remote workers are higher

The pandemic revealed cybersecurity challenges not seen before, or at least not as prevalent. Remote staff need extra training to keep digital assets safe, which means higher cybersecurity costs.

- The costs of employee training are nominal compared to the cost of cleaning up security mistakes.

03

Count on spending money on incident response

It's not a matter of whether a security breach will happen, it's when, Even the most well-prepared organizations aren't immune. Cybercrime shows no signs of slowing down-make sure your budget reflects risk tolerance.

- Ransomware affects 62% of small to medium-sized businesses and 32% of larger organizations according to a 2020 report.

04

Hardware and software will need security updates

The surge in remote work made hardware and software upgrades a higher priority in 2020. As the trend continues, look for outdated equipment and software to be replaced by upgraded security features such as biometrics.

- Unapplied updates and outdated hardware leaves your computer, network, and critical data at risk for cyberattacks and malicious threats.

05

You may need to invest in cybersecurity consultants

Hiring a consultant to help guide security preparedness can save you an untold amount through prevention. A good consultant can help you understand the specific threats you face as well as industry best practices, and can help you gain internal buy in with executive leadership.

- A cybersecurity consultant can help obtain buy in with executives at companies struggling with internal roadblocks.

06

Cybersecurity insurance premiums have increased

IT executives and CFOs aren't the only ones who've noticed that remote employees present a huge risk. Insurance companies have seen the statistics and are charging more. Plan for higher premiums if you already have cybersecurity insurance; if you don't you should seriously consider getting it.

- Cyber insurance premiums, which now total about $5 billion annually, will increase 20% to 30% per year on average in the near future, Standard & Poor's Corp. says.

07

You may need to outsource your cybersecurity program

Outsourcing is a good option for companies that find the costs of running a successful cybersecurity protocol in-house unmanageable. A qualified vendor can take care of your cybersecurity in its entirety leaving you free to focus on strategic activities.

- 83% of IT leaders with in-house security teams are considering outsourcing their security efforts in 2021.

Do you know your company's security vulnerabilities?

Our IT Risk Assessment is a quick, low-cost way to check your cybersecurity posture and thwart potential breaches. For $1,000, our report analyzes:

- √ **Hardware**
- √ **Software**
- √ **Configuration**
- √ **Accessibility**

Protect your organization, your clients, and your reputation

CSH Cybersecurity Services

- √ **IT risk assessment**
- √ **Updating or creating an incident response plan**
- √ **Responding to a data breach**
- √ **Security assessment and testing**
- √ **Penetration testing**

TALK TO A CONSULTANT

CLARK SCHAEFER HACKETT
BUSINESS ADVISORS