Cybercrime Costs
BUSINESSES
AN ESTIMATED
$375-575 BILLION
EVERY YEAR.[1]

Is Your Company Safe?

884 — According to the Privacy Rights Clearinghouse, most data breaches go unreported. Publicly known **IT security breaches total 884 million** records in the US since 2005.[2]

ABILITY TO SUE — Ars Technica confirms: Federal Appeals Court upholds FTC ability to **sue for insufficient data security**.[3]

$578 MILLION — TIME Magazine reports Ashley Madison owners face a **$578 million lawsuit** for a breach of security.[4]

$46.7 MILLION — Fortune Magazine says "CEO Fraud" and **"Business Email Compromise" cost** Ubiquiti Networks **$46.7 million**.[5]

$179 MILLION — The FBI's Internet Crime Complaint Center reports between October 2013 and December 2014, **wire transfer scams cost US businesses $179 million**.[6]

COMMON CYBER RISKS

DATA BREACHES
Confidential information is stolen or removed. Not only does this compromise your company and open you to potential lawsuits, it can put you out of business.

DATA LOSS
Erasing or stealing confidential information, this can occur externally or in-house.

MALWARE
Downloading malicious software through a website, or email attachments can compromise your computer security. Either can slow down your entire network, or can take over your network capacity to run another business, like an online casino.

DATA CORRUPTION
Compromises your IT security by changing vital information such as tax records, budget spreadsheets, a student's grades or any other confidential information you store.

IMPERSONATION
Faking the email of highly placed company personnel. Particularly common is requesting distribution of funds, posing as the CEO or another person in a position to make a request that would not typically be questioned.

VIRTUALIZATION
Running many servers on one piece of hardware makes it possible for a cyber criminal to take down an entire server infrastructure if they get access to the host server.

HOW TO COMBAT CYBER CRIME & PROTECT YOUR NETWORK SECURITY

It may sound dull, but

IT STARTS WITH POLICY.

Create robust policies, complete with an overarching policy defining which policies you need and how often they should be updated. Create a plan for enforcing these policies.

WHAT SHOULD YOU HAVE POLICIES FOR?

PASSWORDS
Include how often to change them, how complex they should be, their length and who to share them with, or not.

NETWORK SECURITY
Including how to set up your firewall and what kind of firewall you need.

ACCESS
Determine who is allowed to access your wireless network. Create audit parameters to make certain only people who have been granted access are using the system.

PATCH POLICY
New security breaches are discovered almost weekly. You must have a policy/method for staying up-to-date and keeping your computers lock-down safe.

LIFECYCLE POLICY
Decide how often hardware and software should be updated and why. Determine how you will dispose of used equipment to protect your security.

ONGOING TRAINING
Decide how you will onboard new staff and make sure they're security compliant. Create a training policy so everyone is always up-to-date.

BACKUP YOUR DATA
Anything can go wrong at any time. Physical damage including fire and theft as well as software and hardware issues can compromise your data. Make sure you have quality backups and review them frequently.

AUDIT & TEST YOUR SYSTEMS
Once you set up security systems, how do you know they're working adequately? Don't wait for an emergency to find out. Regularly test your security and the integrity of your backups

VIRUSES & MALWARE
Make certain each workstation and server has business-class endpoint security software. Malware is very high risk, designed to steal personal information and conduct identity theft. Viruses tend to be destructive, causing data corruption and loss on infected workstations and servers.

Want to Know How Your Company Measures Up?

Request Your Free Security Audit.

No Pressure. Not a Sales Pitch.

Call us Today: 303.383.1627 x1

Misson Critical Systems
IT Support Services Colorado

1. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
2. http://www.privacyrights.org/data-breach?order=field_breach_total_value&sort=desc
3. http://arstechnica.com/tech-policy/2015/08/ftc-can-sue-companies-with-poor-information-security-appeals-court-says/
http://time.com/4007374/ashley-madison-578-million-lawsuit-canada/
4. http://time.com/4007374/ashley-madison-578-million-lawsuit-canada/
5. http://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million/
6. http://www.bankinfosecurity.com/fbi-issues-wire-transfer-scam-alert-a-7846/op-1