Protecting Your Data

The 2024 Cyber-Security Threat Landscape

THE CYBER-security landscape changes constantly. For employers, it's important to stay on top of these threats so that they can ensure that their security protocols and internal procedures are up to the task of beating them back.

Recent reports from cloud-computing provider Google Cloud and cyber-security vendor Netwrix forecast several trends, including:

- **Tighter cyber insurance requirements.** Insurers already insist that their policyholders implement employee security training, multi-factor authentication and security patch management. Netwrix predicts that in 2024 carriers will also require user identity and access management practices.
- **Artificial intelligence will have mixed effects.** Google Cloud says criminals will use AI to make phishing attacks and information-theft attempts more convincing. However, it will also make event response and analysis faster.
- **Theft of encrypted data will become more frequent**. Netwrix says criminals will bet on future improvements in technology that will permit them to eventually unlock encrypted data that is unintelligible today.
- **Criminals will seek out and exploit 'zero-day vulnerabilities.'** These are security holes in software that are unknown to the manufacturer or vendor when it is released. Criminals will look for these weaknesses to infiltrate systems.
- **AI will make criminals convincingly multilingual.** Netwrix expects criminals to use AI to write e-mails in languages other than English and with better grammar. This will make phishing e-mails more difficult for even wary users to spot.
- **Security fatigue will become a greater problem.** Experts and organizations warn users often about cyber-security risks and require frequent training. However, the constant warnings and admonitions about passwords may wear them out.

Users accessing systems remotely may have to enter as many as five or six passwords before they even begin working. Security fatigue can cause user errors that security is supposed to prevent.

WHAT TO DO

These new challenges can seem overwhelming, but there are things individuals and businesses can do to face them:

- Regularly assess cyber-security risks and implement improved mitigation methods to address them.
- Make encryption one facet of data protection, not the only one. Invest in incident detection technologies and create a written plan for incident response.
- Recognize that stolen encrypted data may not be used immediately. Monitor the internet for future use of the data.
- Update phishing training for users so they will be more suspicious of even convincing e-mails.
- Similarly, train non-English speakers on the potential for phishing e-mails in their languages.
- Require users to have unique strong passwords that they must change every three months or less.
- Limit and control the use of system administrator access.
- Tailor awareness training to the needs of specific user groups to avoid overwhelming all users with security information they might not use.

The takeaway

Besides having in place cyber-security protocols, you should also have a robust cyber insurance policy. ❖

Protect Your Business's Data and IP

ASK US ABOUT CYBER INSURANCE