All businesses have a responsibility today.

Centec21 offers information and cybersecurity consultant services, focused on ensuring that small businesses understand their obligations associated with government data privacy laws and respective cybersecurity and regulatory requirements.

Services

- Assessments
- Compliance
- Policy Development
- Awareness & Training
- “Palatable” Remediation Planning
- VCIO

centec21
Information Security

Paul Engelbert
Paul.Engelbert@centec21.com
Cell: 631-495-6493
linkedin.com/in/paulengelbert

Are you truly doing everything you can do to secure your information and mitigate the risk of a security breach?

Cyber & Information Security

Why Cybersecurity Matters – Results of a Data Breach

- **Investigations, fines and remediation.** If a breach involves payment-card data, you'll face substantial fines from the card brands. Why? Because all card acceptance agreements require you to remain compliant with the Payment Card Industry Data Security Standards. Breaches cost the average small business between $36,000 and $50,000. Fines alone for major breaches can far exceed $500,000.

- **State breach-notification laws.** Each state has its own law governing how you must notify customers of a data breach. All the laws are slightly different, which can make compliance difficult for multi-state operators. The Association has lobbied Congress to enact a single federal statute, but Congress has yet to act.

- **Class-action lawsuits.** Breach notification typically triggers class action suits, and customers may be able to sue simply based on the risk they face following a breach. Even a suspected breach can trigger legal actions and negative press. Costs can add up quickly.

- **Brand damage.** Damage to your reputation and the loss of customer loyalty can severely impact your bottom line after a breach.

Cyber & Information Security

Data Breaches – How do they occur?

Hackers can obtain access to your network in various ways, but the most likely approach is through a successful phishing email attack. Once they obtain access to your network, they usually lay dormant or passive for a period of time.

- While Passive: Hackers move laterally across your network, obtaining an understanding of the infrastructure.
    - Priority Targets and objectives:
        - Privileged Accounts (enable access to critical systems and sensitive data)
        - Backup servers and locations
        - Sensitive/confidential data locations
        - Critical network devices
- While Active: Hackers execute the Breach.
    - Locking out Privileged Accounts (e.g. backups, admins)
    - Applying unknown encryption to backup data and production data.
    - Shut down or lock users out of critical systems.

Cyber & Information Security

Incident Response – Things to Consider

- Do you know who will be affected by a breach? (i.e. customers, employees, suppliers, etc.)
- Do you know what your legal requirements are? (i.e. data privacy laws, notification, etc.)
  - Know what to say, how to respond?
- Do your current contracts set any additional legal obligations in the event of a breach?
  - Is data shared with third parties or stored in nonintegrated systems secured?
- Do you have cyber insurance?
  - Provides liability protection
  - Provides cyber security company for breach response.
  - Provides a breach coach/attorney
    - Offers autonomy via attorney client privilege
    - Manages breach response and remediation.
- If no cyber insurance;
  - Do you have an attorney you can consult who know about cybercrime?
  - Do you know who to call should a breach or incident occur?

Cyber & Information Security

Awareness & Training

centec21 Information Security

Training	Details	Min Cycle	Cost
General Security*	Password, Acceptable Use, Safe Web Browsing, Ransomware, Social Engineering	• Upon Onboarding • **Yearly**	$20-$30 Yr. (per user)
Phishing	How to identify and act on phishing emails.	• Quarterly • **Yearly**	$10-$15 Yr. (per user)
PCI	POS/Retail – Handling CC Data	• **Yearly**	$15-$25 Yr. (per user)

Your greatest threat and weakest point of entry to your business is yourself, and your employees.

- Cyber & Information Security Awareness is a businesses first line of defense.
- Enforcing employee training "will" greatly reduce the risks of a security breach.

Scientiapotentiaest – *"Knowledge is power"* Sir Francis Bacon.

*Type of training should be based upon role and required data accessibility.

Cyber & Information Security

Recommended Security Best Practices - General

centec21 Information Security

Control	Impact
Ensure up-to–date patches and versions/service packs (i.e. antivirus, operating systems, software, etc.)	M-H
Training staff on your data security policies and/or business requirements.	L
Limit access to information, data sources and applications through explicit user roles and passwords. (Need to know, control access)	M
Disable default, admin account, dormant user accounts and un-necessary service accounts.	L
Change user passwords periodically based upon role (Use complex passwords (12 Char. Min) or us passphrases of 15 Characters or more. (Use password vault)	M
Implement steps to protect your most sensitive data. (i.e. encryption, network segregation, etc.)	L
Know where your sensitive/critical data is and who has access to it.	L
Obtain Cyber-Insurance (Do sooner rather than later; starting to impose criteria before underwriting policies)	L
Use Multi-Factor-Authentication (MFA) wherever possible.	L
Verify Contracts – Privacy, IR	M
Ensure Daily Backups, including backup protection (i.e. encryption, access control), and maintain physical backups.	L
Implement network security best practices. (i.e. segregation, FW, VPN, MAC Filtering, Static Ips, etc.)	M
Conduct yearly pen tests.	M