Data leaks, disasters and what to do

Data leaks are damaging. It’s never too late to put ten basic security practices in place.

52% of firms* in Ireland have no comprehensive strategy when it comes to preventing digital crime or data leaks.

Sensitive data leaks are the stuff of nightmares for business owners (and public representatives). What can you do when the horrible happens?

When it comes to sharing information, social media strategist Darragh Doyle says business owners should have very clear social media policies in place.

“Along with the policies and a nondisclosure agreement, employers should make it very clear that company information is never published in social groups,” says Doyle.

Nightmare scenario

And what do you do if customer data or other sensitive data makes its way into the ‘wrong’ hands?

“You have to own the problem,” says Doyle. “You have to find out how the issue occurred, where did it leak from, and then seek to address the fallout.”

Can someone press the big red button?

“You also need to know the administrators of your social media groups and trust them. The question is, ‘Can someone hit the big red button?’" asks Doyle.

Data dumps

It’s also important to keep company devices free from sensitive data. “Employees should be asked to do a data wipe, every day if necessary,” advises Doyle.

“For example, they may have downloaded a database for a meeting to view it on screen. They should erase sensitive documents. It’s like having a clean desk policy but for smart devices and laptops.”

The top ten things to do

*Grant Thornton suggested in a 2016 report that only 16% of Irish firms *believe* that cyber-crime is a credible threat.

The cost of cyber-crime to the Irish economy is estimated at €630m annually.

Here is a list of 10 useful tips that will help protect your business from cybercrime.

- **Secure your computers:** Firstly, install anti-spyware and anti-virus software and always make sure that your firewall is activated. Additionally, Windows has a standard firewall on all of its computers. Access it from your control panel and confirm it’s switched on. This will help reduce your susceptibility to malware.

- **Secure your wireless network:** Verify that your wireless network is not available to the public. Verify that your internet access is password protected and restrict usage to employees and guest visitors.
- **Encrypt your data:** Encrypt, encrypt, encrypt. This cannot be emphasised enough. Encryption allows you to encode your information so that only authorised personnel can access it. Use encryption for any sensitive files or data that you own.
- **Avoid clicking unsafe links:** The old saying “if it sounds too good to be true, then it probably is” rings true here. Exercise caution when it comes to advertisements online, install ad-blocking software or, better yet, simply ignore them.
- **Use strong passwords:** Perhaps the most obvious safety precaution, you should implement a strong alphanumeric password policy that consists of numbers, lowercase letters, uppercase letters and special characters with the password requiring a minimum of 12 characters.
- **Review statements regularly:** A relatively simple action, review your monthly financial statements and check for any irregularities. If you spot anything suspicious, contact your bank immediately.
- **Keep systems updated:** To combat any new threats that may emerge, keep your anti-

virus software and Windows systems up-to-date. Advise staff to update their systems on a regular basis. If this approach is not suitable, automate how your updates are installed and roll it out across the whole business.

- **Social media housekeeping:** Make sure there is adequate security surrounding who has access to the company's social media accounts. Ensure that only authorised personnel have access to social media accounts and the log-in details.
- **Use multiple email accounts:** Use a separate e-mail for financial dealings, another for social networks and one for general queries and so on. In the scenario that a hacker manages to gain access to one of these, all of the sensitive information isn't compromised. In the same vein, use different passwords for each address.
- **Don't store your credit card information online:** Yes we know it's a nuisance but having to input your card information for every transaction can save you a lot of hassle in the long term. If a hacker does manage to bypass your security they may also have access to your card details. Don't take the risk. Alternatively, only use a prepaid card online.

If you find yourself the victim of a cyber-attack please contact The Garda Bureau of Fraud Investigation on +353 1 666 3776 as well as the Data Protection Office and your Internet Service Provider.