What Senior Executives Need to Know About Cyber Breach Management

Senior executives are justifiably concerned about cyber risks and the need to recover quickly and safely if their organisation is hit by a breach. But what involvement should they have in order to help make the business more resilient, and a recovery more successful? If you think all you need is cyber insurance, then please read on…

Colin Jeffs, Head of BCM Consultancy at Daisy Corporate Services, explains the difference having an overall strategy for resilience, sponsored at board level, can make….

If you sit on the board of directors, you need to know that there's a comprehensive plan in place that covers exactly what happens when a cyber breach hits, and you need to know that there is a defined reporting structure that keeps the flow of information and decision-making around the incident management and the recovery effort, open and effective.

It is common for one board member to have overall management of risk, but an important part of achieving resilience should be communication and decision-making relating to risk, across the full board of directors. It is really important for all senior executives to be prepared, and this means having high-level knowledge of the plan, and doing your part to shape the strategy.

Here's why it's so important if you are a C-level executive:

1. **You are responsible** – as a member of the board of directors, it is your responsibility to ensure that the area of the business that you oversee is resilient and has appropriate plans in place to manage any business interruption. Being active in the strategy ensures you have this covered for your area.
2. **You are accountable** – as far as regulators and the law is concerned, accountability for any resulting loss of data and the penalties associated with that, starts with the CEO and the company board of directors. It is literally in your own best interests to ensure the correct processes are in place for data protection.
3. **You are visible** – internally and externally, you are a known representative and policymaker for your business and as such, you set the expectations for resilience both internally for your staff to follow and externally for the peace of mind of your customers and supply chain. Your involvement in the planning and execution of the strategy raises the profile and the focus on resilience, helping to embed resilience internally and send all the right messages externally.
4. **You are vulnerable** – last but by no means least, board level executives are prime targets for cybercriminals. Not only do you have great access within your organisation, but you also have access to the most high-level and valuable company secrets and are more likely to have influential contacts and reach within your industry sector. Being part of your planning means you are more aware and alert to the potential risks and how to keep safe.

Top board-level action points

I recommend three over-arching steps that are overseen at director level. These steps will help to embed a resilient culture throughout the organisation and ensure the business can bounce back or avoid major impact altogether following a cyber breach and naturally, disruption from other causes:

1. **Establish unified ownership across your resilience staff**

Make sure there are clear reporting lines and decision-making processes relating to cyber risks and cyber breach management. This needs to include business continuity, information security, risk management, and IT. It's important to remember that resilience incorporates and transcends all of these areas.

2. **Promote information sharing**

Internally: to understand what the cyber threats to your organisation are and how they are changing. Externally: to exchange intelligence across your industry sector and business network to help identify and manage emerging threats.

3. **Promote your information security policy**

Ensure there are processes in place so that information security is understood by all staff and supported by regular staff training. Most cyber breaches occur because a member of staff has clicked on something they shouldn't have or opened an email and attachment that they were not sure about. And if you are still not sure that resilience needs to have such a big focus on your corporate agenda, there are some compelling benefits:

Business benefits
Digital transformation or any change in the way your organisation functions needs an element of risk management to be undertaken. A focus on resilience at the heart of your decision-making is critical to your continued success, understanding and mitigating threats, identifying opportunities, and ensuring confidence in your strategic direction.

Operational benefits
Every boy scout will tell you that you should be prepared. When you are prepared for the unexpected in business, you are not only more likely to endure any setbacks, but you have a culture that means that relationships, dependencies and processes are understood at an intrinsic level. This not only drives innovation and productivity, it ensures decision-making does not occur in silos.

Financial benefits
Greater productivity from more collaborative working is a natural result of a resilience-first approach and provides welcome financial benefits. But there are more tangible benefits including the continuation and potential reduction in insurance premiums, that come from having cyber secure backups in place, for example, And don't forget, the reduction in losses and downtime and the peace of mind for your customers and the market you operate in won't harm your sales potential either! Remember that customer and market confidence is everything in business and if the market has confidence in your business because you've shown you have resilience in place, you are far more likely to ride out any storm.

So, the best way to take your business forward, is to keep resilience at the heart of everything.

About Colin Jeffs MBCI

Colin moved into the realm of business continuity from IT project management where, as part of implementing IT systems, he had to implement resiliency. Colin has worked in business continuity and crisis management for more than 25 years, holding senior roles in both disciplines for many years at major financial institutions in the city. Colin now heads up Daisy's award-winning business continuity management division.