



Why an incident response plan may be your best business investment this year

[Leave a Comment](#) / [Security](#) / By Jason Buckley

It's a bold claim. You probably have many ways you're investing in your business this year. Perhaps you've hired more staff to help you scale, bought some promising new equipment that cuts costs, or hired a PR rep to improve your public image. But what if there was an investment that could do all three of these things at once? An incident response plan is an IT solution that can: better your reputation, scale your company, and reduce your expenses. But before explaining how it does this, you may be wondering...

What is an incident response plan?

An incident response plan is a set of processes your staff follows in the event of a security incident. These instructions include how to detect the incident, respond to it, and mitigate your losses. It's similar to disaster recovery and business continuity plan but focuses specifically on cyberattacks or network security issues. Its goal is to reduce data loss and downtime, which ultimately can benefit your business in many ways.

Benefits of a cybersecurity incident response plan

While there are many benefits to an incident response plan, below are three that can serve as a catalyst for business growth while protecting you from cyber attacks.

1. Reduce your business expenses

If a cybercriminal infiltrates your business, can you continue operations? Similar to a business continuity plan, an incident response plan's purpose is to keep your lights on, regardless of the type of breach experienced. This ensures that downtime is minimal, and you limit the losses from staff being unable to work. The truth is, security breaches are increasingly common. According to the [2020 Thales Data Threat Report](#), 49% of American businesses have experienced a data breach. So preventing them can save you a lot of money in the long run.

Incident response plans require documentation of your processes, which often includes taking an inventory of your current equipment. During this inventory, your team may uncover redundancies and faulty equipment. For example, you could discover that you really don't need three servers, one may be enough. Or you may learn some of your computers have viruses, which have been causing slow performance and unexpected shutdowns. Resolving these issues can save you money and provide added security.

2. Improve customer and employee confidence

A security breach can be devastating for your business's reputation. While notifying your customers of the incident can be embarrassing, it also breaks their trust, as does the downtime you experience that disrupts their service.

One of our clients faced just such an incident when they suffered a [security breach](#) in 2016. The owner accidentally installed a ransomware program. While the ransom our client paid was only \$1,900, three days of downtime and telling his clients about the breach were much more costly in damage to the company's reputation and loss of employee productivity. Had our client had an incident response plan, they would have had a backup that could have restored the company's data and operations that day.

Incident response plans are essentially an investment in your business's credibility. You gain the trust of your clients, partners, and employees. You can promote your security measures or track record in your marketing, which can bolster customer confidence and drive leads. Lastly, if your business must follow HIPAA or other industry regulations, an IT incident response plan can help you stay compliant and avoid fines.

3. Scale your business

While incident response plans typically involve an inventory of your equipment, they also can include a review of your network management. This documentation process could identify roadblocks to your growth, such as outdated technology.

For example, perhaps you've been using slow internet service and weren't aware of it until now, or maybe you decide to migrate from local backups to cloud backups, which simplifies your data maintenance process and reduces costs. In either scenario, your staff could save dozens of hours a month, which frees up their time and improves their efficiency. Ultimately, the documentation process can help you modernize your business, which in the long run will only provide you better, faster technology that accelerates your growth.

An incident response plan is critical to any business's success

An incident response plan is really much more than an investment in your business. While the time taken to improve your processes will pay dividends in growth, you also bolster your reputation and protect your operations from cybercrime—both vital to the survival and success of your business.

If you need help creating an incident response plan, don't hesitate to contact Jasco. Our team of IT professionals will look for ways to cut costs, optimize your processes, and prepare your business for potential security breaches. [Contact us today](#) to learn more.

[← Previous Post](#)

[Next Post →](#)

Leave a Comment

Your email address will not be published. Required fields are marked *

Type here..

Name* Email* Website

Save my name, email, and website in this browser for the next time I comment.

I'm not a robot

POST COMMENT »

Search...

Recent Posts

- [The essential incident response checklist: 21 steps to navigating a cyber attack](#)
- [Why an incident response plan may be your best business investment this year](#)
- [Why IT strategy is important for SMBs](#)
- [Understanding IT support costs: Is it worth investing in managed services?](#)
- [Five reasons to move to managed IT services](#)

Recent Comments

- [Shammy Peterson](#) on [How to ensure your practice benefits from telehealth](#)
- [ICTechnology](#) on [Understanding IT support costs: Is it worth investing in managed services?](#)
- [globalmdplus](#) on [What is telehealth?](#)
- [Chris Q](#) on [Real world examples of security breaches from Las Vegas companies](#)

Archives

- [June 2021](#)
- [May 2021](#)
- [April 2021](#)
- [March 2021](#)
- [January 2021](#)
- [December 2020](#)
- [November 2020](#)
- [October 2020](#)
- [September 2020](#)
- [August 2020](#)

Categories

- [Business](#)
- [Healthcare|Security](#)
- [Managed IT Services](#)
- [Security](#)