Research Report 2018

2018 Legal Business Continuity Survey

The risk of disruptive events on business continuity for law firms

This report includes data surveyed from more than 50 law firms on both sides of the Atlantic to better understand how prepared they are for significant business outages.

Instant
RETHINKING WORKSPACE

Sandpiper Partners LLC

Contents

Introduction....4

When disaster strikes…....5

What is the biggest threat to the legal sector?....6

The implications of cyber security....10

Working during a natural disaster....12

How long should you plan to be without your office for?....13

What have law firms learned from regular testing?....16

What happens next?....17

Appendix....18

Introduction

The survey was conducted in partnership between The Instant Group, a workspace company that works with some of the largest law firms in the world, and Sandpiper Partners, a consulting firm and conference organizer with expertise in the legal sector.

The research asked firms to comment on their capabilities to service clients' requirements in a period of business outage and planning in this area.

The majority of firms seemed confident that the necessary business processes were in place, but their responses also hinted at the lack of consistency in their approach to BCP and much of the procedures remain untested.

In particular, many firms' plans are dependent on remote working and IT processes that have, in several recent cases, been put at risk during natural disasters or acts of terrorism.

When disaster strikes…

This research was commissioned in response to 2017's cyberattack on a major law firm that affected its offices in New York, London and Europe.

> **"It's a nightmare… ransomware attacks sound cybersecurity alarms for law firms,"**

one legal journal headlined after a large Global 100 firm was shut down worldwide (in late June) for three days after an attack.

Not only could a company-wide disruption happen—it did happen. And this situation – and the ability to service clients during an outage – now presents a significant risk to all firms.

Law firms operate in a world where clients expect them to be prepared at all times to function without disruption—regardless of a cybersecurity attack, terrorism, natural disaster, data breach or emergency at an office facility. But there is a large gap between what clients consider readiness for such a situation and the reality of how widespread a cyberattack can paralyze a firm in every aspect of its operations from telephones to computers.

There are several key areas for consideration across workspace, IT and HR that all need to be addressed within the context of business continuity planning. Understanding how to co-ordinate the approach across these business areas is fundamental to a firm's ability to minimize the disruption caused by a business outage of any size. However, what this research brings to the fore is the need to be adaptive and flexible in response.

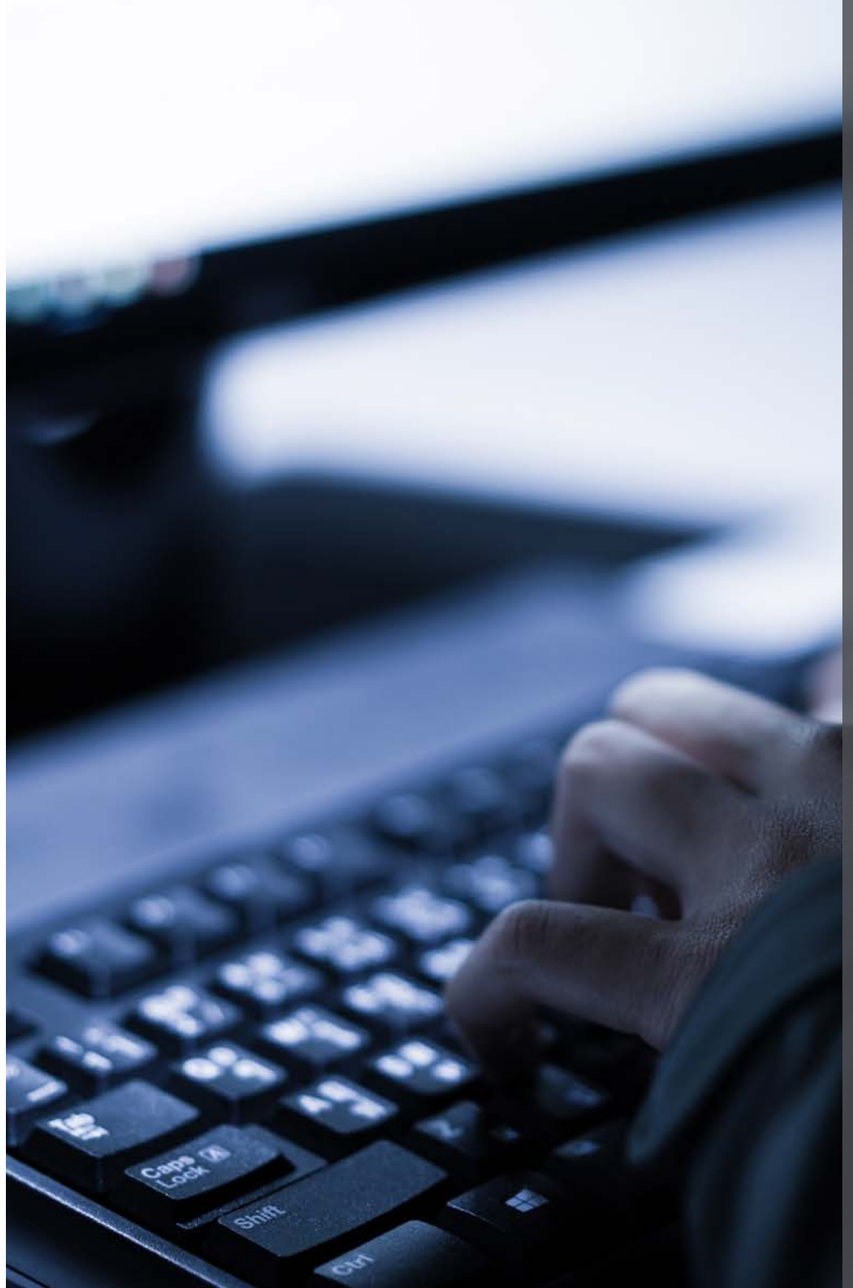
Our research assesses these different areas of co-ordination and also includes information from experts in key issues such as cyber-attacks and other future threats to business.

What is the biggest threat to the legal sector?

The majority of replies to our survey expressed confidence that they would not have a problem. Some of the replies demonstrated the respondents faith in their current systems:

> Minimal impact to client service
>
> **Full service**
>
> Hopefully, business as usual
>
> **We expect to be able to continue to provide the service to the clients as per our SLAs**
>
> Service would remain. All of our staff can work remotely & we can use alternative space to hold meetings
>
> **Everyone in the firm can access our systems remotely either at our primary or back-up sites, so our ability to serve clients would be unaffected**
>
> We have plans in place to be able to continue to service our clients
>
> **High assuming ongoing access to internal network**
>
> Materially undiminished

Given some of the very high profile business outages resulting from Ransomware in the past year these responses show a remarkable degree of confidence. Disruption can come in many forms, but **71%** of the firms perceive data breach/cyberattack as the number one threat. Accordingly, technology disruption replacement (**78%**) is the BCP service that has the greatest priority.



How could an outage affect law firms?

The top three effects are revenue loss (**74%**), inaccessible or lost data (**71%**) and reputational impact (**63%**). From anecdotal responses, our respondents believe that an IT outage might only affect their business for one hour and that staff would be able to "work remotely to continue servicing clients." These responses place an enormous amount of faith in cloud computing, the security of these services and the sources from which staff can login from.

Who has responsibility at law firms during an emergency?

Law firms have a variety of people who have been assigned responsibility to supply information on this topic. Most commonly, **40%** said they were C-level executives. But others had more than 20 different titles ranging from Risk and Business Continuity Manager to General Counsel.

The importance of a BCP

Virtually all firms now place a high priority on BCP. We found **98%** of firms have a BCP in place. Clearly, the top concern is IT functions with **77%** reporting they have a separate BCP plan for IT, **57%** for communications, and **51%** for human resources. Plans are in place by over **two thirds** of the firms for both staff and clients. As for responsibility for BCP, **22%** of the firms say the CISO/Director of Information Security is responsible for their BCP and services, while **19%** state it is the COO who has these duties.

The disparity between different legal firm's approaches to BCP is telling as it demonstrates that knowledge in this area sits across numerous different areas of expertise. Increasingly, HR, IT, operations and even communications have strategic overview of BCP priorities.

Why is IT such a significant area of concern?

With the cyber-attacks that have affected firms of all types over the past year, highly technical IT issues have seen communications and facilities unravel rapidly in a short period of time. This situation has been amplified by the inability of the relevant teams to communicate around the issue at stake.

For example, **more than half** of firms we surveyed operate data/document storage onsite and manage this function onsite, a potential serious vulnerability in the event of a disruption.

More than **70%** of the firms included remote working as part of their BCP.

The utilization of remote working, while seeming a sensible solution also opens up risk of further complication as it works on the assumption that mobile networks and cloud computing remain robust and secure.

As last year's attacks demonstrate, firms should plan where possible to allow staff to congregate and for clients to meet in a safe and secure environment.

The implications of cyber security

Cameron Colquhoun,
Managing Director of Neon Century Intelligence, a leading London-based security firm

Future-proofing

With a shortage of cyber skills in the business and legal profession in particular, the sector often looks to the past to manage the risks of the future.

However, in cyber-security, this way of thinking can lead to businesses investing in the wrong strategy or security products. Cyber threats are continually evolving and businesses suffer from a creativity deficit when it comes to imagining how a crippling cyber-attack could arise.

Cyber risks

One trend over the last 12 months is the growing scale of cyber-attacks, three high profile events in 2017 highlight this:

In March, hackers gained access to all of Deloitte's cloud data, effectively able to access every part of the corporation and its sensitive projects. In May, the WannaCry virus plagued the UK's NHS and many other organizations, leading to disruption for hundreds of thousands of people, and in August, US data giant Equifax was hacked, with personal data from 200 million people leaked online.

This scale trend will continue. Critical business functions – electronic door access, cloud storage, point-of-sale systems, logistics software, are each in their own way increasingly vulnerable to large-scale cyber disruption. As companies automate their key operations, few realize the inherent trade-off between efficiency and cyber risk.

Consequences

A second business 'blind' spot arises in the world of geopolitics and cyber security. The next war between a western country and an adversary is very likely to lead to large scale cyber disruption in the West, with unknown but potentially huge consequences for the economy and business continuity. North Korea and Iran have very advanced cyber-attack capabilities and unconstrained by geography, would undoubtedly wreak havoc from New York to London to Singapore.

For example, during a period of tension with Saudi Arabia in 2011, Iran launched a cyber-attack on Saudi Aramco, wiping 30,000 computers in a keystroke. It is sobering to realize that this occurred in peacetime. Few businesses acknowledge that a war, thousands of miles away, could have a direct impact on their ability to operate.

Therefore it is imperative that businesses begin to think about the signals, or warning signs, that may trigger a crippling cyber-attack. This includes proactively monitoring other cyber events, stress-testing internal systems and wargaming the possibility of operations without electronics and the internet. In this way, cyber is similar to other forms of risk: prepare for the worst, and hope for the best.

Communicating with staff during a business outage?

The preferred choice of the vast majority of firms for emergency communications with staff is email or SMS.

More than 89% would choose these channels for communicating with staff in case of an emergency but again, this is based on the assumption that the networks supporting these communication options remain viable.

Third party messaging apps (WhatsApp, Skype IM, etc) came in second with **71%**.

Continuity plans for office space are in place, according to many of the companies surveyed. **85%** percent of firms say they have a contingency plan if their office space became inaccessible tomorrow for an indefinite period of time.

And flexible offices are a growing part of plans. A slight majority of firms (**53%**) leverage flexible offices as part of their BCP strategy and **36%** state flexible working space and space agility is a high priority. More than **70%** of the firms included remote working as part of their BCP.

Working during a natural disaster

Many businesses may be equipped for a cyber-attack – however lack an adequate business continuity plan in the event of a natural disaster.

Weathering the storm

For example in Houston, Hurricane Harvey left over 248,000 with power outages, inclusive of commercial properties, with many of these businesses lacking the means to continue operating, and opting for home-working instead.

Alternatively, one local company used Air BnB to set-up a temporary office for workers during the hurricane; the flexible space allowed employees to be close to the office as well as in a comfortable environment to continue to work throughout the storm.[1]

They also resorted to 'SIP trunking' to ensure they remained connected and were able to continue working throughout and after the hurricane.[2]

However many of the businesses affected lacked a contingency plan and resorted to 'remote working' resulting in further loss of productivity.

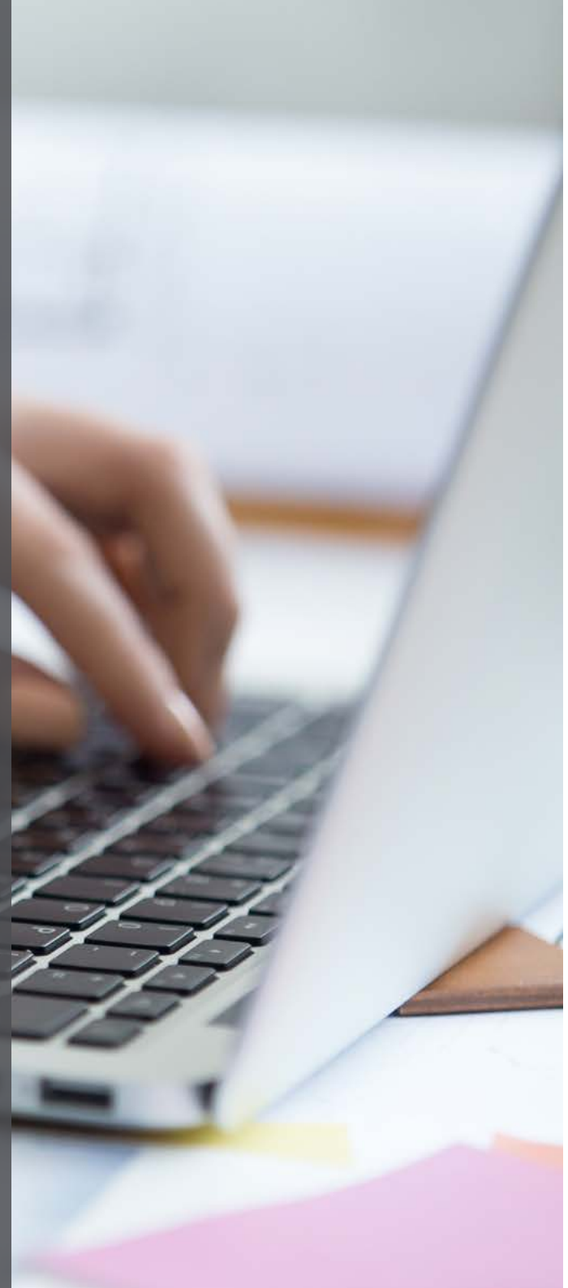
Preparation is key

It was law firms within the area that prepared ahead of time; they ensured their co-location facility was aware of any impact to their work as well as ensuring that an off-site help desk provider was available meaning the impact of the storm did not impact the service to clients.[3]

Similarly in Puerto Rico there were significant damages and consequently displacement for businesses with most of the electrical grid still being wiped out over a month on, with reports that full electricity might not be back for over a year.[4]

Sources at the scene said that businesses were on a race against the clock if emergency power supplies ran out – implying that once these ran out there could be a complete shutdown.[5]

1 Source: https://answeringservicehouston.com/strategies-to-keep-business-running-during-a-natural-disaster/
2 Source about SIP in disasters: http://sip-trunking.tmcnet.com/topics/sip-trunking/articles/337132-sip-trunking-disaster-recovery-business-continuity.htm
3 Source: http://www.benefitspro.com/2017/09/01/tech-lets-houston-firms-work-despite-hurricane-har
4 Source https://www.bloomberg.com/news/articles/2017-10-29/hud-explores-temporarily-housing-puerto-ricans-on-u-s-mainland
5 Source: http://uk.businessinsider.com/r-puerto-ricos-fragile-economy-dealt-new-blow-by-maria-2017-9?r=US&IR=T



How long should you plan to be without your office for?

Unfortunately the majority of disruptions tend to affect businesses for **7 days +**, leaving those without real estate contingency at the mercy of an often volatile market to secure 7-28 days space.

Firms leveraging the flexible office market are able to expand and contract their space accordingly and suffer less downtime and loss of productivity than firms who are trying to make their 1 day solution work for a period of weeks if not months.

Fixed, syndicated space provides a mirror of a firm's office, but cannot support multiple locations if a multi-region issue occurs (as with the multiple Ransomware attacks witnessed in 2017).

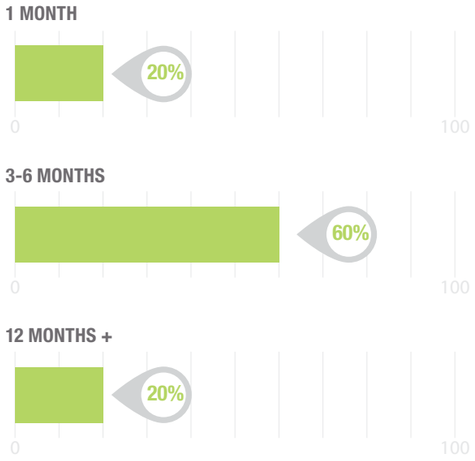
Given the number of subscribers using their offering, syndicated seats might not be available if an event was to deny access for an entire district (ie the City of London). Flexible contingency allows multiple locations and size to be identified and leveraged so the recovery space is closer to employees' homes, or avoids the high profile areas that often suffer attacks, etc.

We surveyed five major operators of flexible workspace to assess how market demand has changed for BCP space, and whether businesses are now looking to serviced offices and co-working centers as viable back up plans.

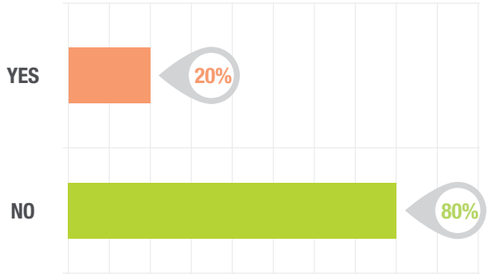
Of these companies – including WeWork, LEO, Halkin, i2, and Orega, which operate centers around the world – all had discussions with large corporates around their contingency plans for natural disasters or IT outages. On the whole, these plans were focused on re-housing a team of 50 to 100 members of staff, so a collection of key workers, and to do so for between three to six months.

The majority of these workspace operators had seen inquiries such as this increase over the past year as firms make further preparations for business continuity during a crisis.

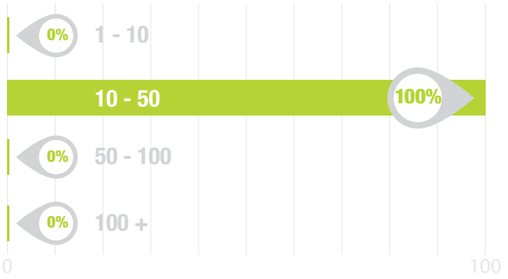
HOW LONG WAS THE SOLUTION ACTIVATED FOR?



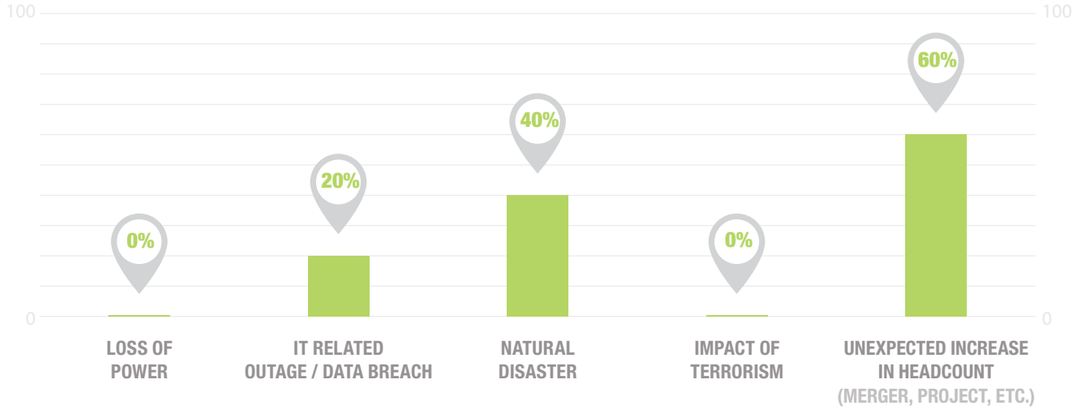
DID THE CLIENT HAVE A BCP(BUSINESS CONTINUITY PLAN) IN PLACE?



HOW MANY DESKS HAVE THESE INQUIRIES TYPICALLY BEEN FOR?



HAVE YOU SEEN AN INCREASE IN INQUIRIES FROM CLIENTS DISPLACED BY EVENTS OUTWITH THEIR CONTROL?*



*Multiple choice question

HAVE YOU SEEN THIS TYPE OF INQUIRY INCREASE IN THE PAST 12 MONTHS?

What have law firms learned from regular testing?

Most firms regularly test their readiness plans. Over three quarters (**77%**) of firms say they have conducted an internal BCP audit or contingency test run in the last 12 months. There were a large range of answers on how long their BCP would be effective; **38%** say the BCP can cover them for over one month of displacement or outage while **35%** are only covered from 1- 5 days. The latter figure is obviously of concern as recent cyber-attacks including the Ransomware attacks known as “Bad Rabbit” and “WannaCry” have affected IT performance for several days after detection and an unknown period prior to that.

In recognition of the threat that these attacks pose, the key priority for firms are technology disruption replacement (**76%**), while facility emergency solutions are a distant second at **52%**. While extreme weather events such as the 2017 flooding in Houston remind us of the importance of an alternative facilities plan, the issues related to cyber-attacks make remote working impossible.

Law firms of course place clients at the center of their concerns in an emergency with **85%** of contingency plans focusing on better risk management and client benefits. Some of our respondents highlighted the importance they place us client-centric planning:

> **“...given that our services are personal in nature, we have located off site data centers in two different US regions that back each other up, geographically distributed offices and good remote working capabilities.”**

What happens next?

The Instant/Sandpiper research has proved useful insight into the existing planning around BCP for law firms but also some of the inherent risks that remain.

An overreliance on remote working, and the assumption that remote working solutions, which focus heavily on mobile comms, would leave many firms exposed to major network outages. A focus on IT solutions rather than effective facilities alternatives in relevant locations would also inhibit the ability of staff to congregate, and put in place client-management strategies and ongoing communication.

Lastly, the different responsibilities that sit across the business from comms to IT, HR to facilities mean that there are a lot of different stakeholders that require consultation. In an emergency, speed of thought and clarity of communication is important with consideration to both internal and external stakeholders.

While the number of legal firms in both the US and Europe with BCP plans in place is impressive, there remains questions about their potential cost of downtime and their approach to emergency re-location and the issues that come with it.

Given the potential cost ramifications it is noteworthy that only **40%** of firms say they receive discounts in insurance premiums for having a BCP in place. As cyber-attacks and extreme weather events occur with increasing regularity, a broader industry response must be put in place and recognition from suppliers to the market such as insurance firms and IT suppliers would be a critical part of this.

Appendix

BCP Context – comparing the legal sector to other areas of business

In 2016 alone, 31.1 million displacements occurred due to conflict, violence and disasters, which is the equivalent of one person forced to flee every second; the number and scale of catastrophic natural disasters is on the rise; 2016 was the hottest year on record to date; cyber-attacks are becoming increasingly sophisticated - global spending on cybersecurity is likely to exceed $1 trillion by 2021.

According to the Federal Emergency Management Agency, more than **40%** of businesses never reopen after a disaster and for those that do, only **29%** are still operating after two years. Despite this, up to **41%** of businesses have no continuity plan in place, and only **34%** are confident that their organization would be able to continue in the event of a disaster.

One of the most comprehensive surveys was completed by IBM and Ponemon, incorporating 383 companies in 12 countries.

The results noted that $4 million is the average total cost of data breach and there has been a significant, **29%** increase in total cost of data breach since 2013.

The study, incorporated 383 companies located in the United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (United Arab Emirates and Saudi Arabia), Canada and, for the first time, South Africa.

All participating organizations experienced a data breach ranging from approximately 3,000 to slightly more than 101,500 compromised records.

They also identified seven global mega-trends resulting from data breaches (they have surveyed 2,000+ companies dating back to 2015).

Seven global mega-trends

1. Since first conducting this research, the cost of a data breach has not fluctuated significantly. This suggests that it is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies.

2. The biggest financial consequence to organizations that experienced a data breach is lost business. Following a data breach, organizations need to take steps to retain customers' trust to reduce the long-term financial impact.

3. Most data breaches continue to be caused by criminal and malicious attacks. These breaches also take the most time to detect and contain. As a result, they have the highest cost per record.

4. Organizations recognize that the longer it takes to detect and contain a data breach the more costly it becomes to resolve. Over the years, detection and escalation costs in our research

5. Regulated industries, such as healthcare and financial services, have the most costly data breaches because of fines and the higher than average rate of lost business and customers.

6. Improvements in data governance programs will reduce the cost of data breach. Incident response plans, appointment of a CISO, employee training and awareness programs and a business continuity management strategy continue to result in cost savings.

7. Investments in certain data loss prevention controls and activities such as encryption and endpoint security solutions are important for preventing data breaches. This year's study revealed a reduction in the cost when companies participated in threat sharing and deployed data loss prevention technologies.

Emphasis on business continuity is vital, and the ability for companies to deliver critical functions uninterrupted during a crisis is invaluable, as is the ability to remain agile in the face of ever-changing threats. With global awareness increasing, organizations investing in their own resilience are looking to the latest trends to ensure preparedness.

Source: https://www.ibm.com/security/infographics/data-breach/

Major Business Continuity Trends

Location strategies: Companies are looking to alternate site locations that are not just geographically distant, but also reliant on different infrastructures. In the event of widespread disasters, the ability to operate from a different electrical grid is important. This is just one example of how vital the choice of location is.

Office space: Not all employee homes are suitable for home working and enabling staff to work from wi-fi enabled coffee shops long-term simply isn't sustainable. That's why, in the event of a crisis, more companies are looking to the convenience of fully equipped flexible workspaces which enables the relocation of employees at a moment's notice.

Integrated solutions: Gone are the days when corporate real estate took care of buildings, IT took care of tech and management dealt with resources - today's business continuity plans require coordination and communication between departments to be effective. In addition, businesses are considering their global interconnectivity far more by not just preparing disaster plans based on local priorities, but by focusing on the global picture with an end-to-end solution.

Internet of Things (IoT) Security: In an increasingly connected workplace, internet-connected devices are found everywhere from staff desks to the company kitchen. As a result, more companies are investing in 'Internet of Things security protocols' such as data encryption to and from internet devices brought in by employees, device authentication procedures and blockchain technology networks for more secure interconnection of devices.

About this report

Sources

https://www.unisdr.org/we/inform/disaster-statistics

http://www.preventionweb.net/publications/view/51602

https://www.nasa.gov/press-release/nasa-noaa-data-show-2016-warmest-year-on-record-globally

https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

http://www.continuitycentral.com/index.php/news/business-continuity-news/1921-the-business-resilience-survey-2017

https://www.ibm.com/security/infographics/data-breach/

The Survey - Three out of four respondents are from a law firm with over 1,300 employees. Another **15%** have 700 – 1,000 and **5%** have 1,000 -1,300 employees. Principal offices of the respondents were ranked in this order, (1) London, (2) New York, (3) Washington D.C. ; the Survey responses also included firms from Chicago, Philadelphia, San Francisco, Los Angeles, Seattle, and Boston. Three quarters of respondents place an international city as one of their top three principal offices; **63%** of respondents operate over 10 locations in the U.S., while **90%** operate between 1-5 in the U.K. Of these firms **97%** report between one and five of those locations are dedicated back office or service centers.

Rethinking Workspace.

We are a workspace innovation company that enables our clients to navigate continual disruption with continual transformation.

Our proprietary, intelligence-driven approach creates flexible workspace solutions that drive growth, inject agility, strengthen brands, attract talent, nurture collaboration, reduce cost, and drive EBIT performance.

With 10 offices globally, we have access to more than 10,000 buildings across more than 1,500 cities and 113 countries, and Alex Milner, Director at The Instant Group, helps companies set up their BCPs, enabling them to get back to business as usual and quickly as possible.

United Kingdom HQ
The Blue Fin Building
110 Southwark Street
London, SE1 0TA
Tel: +44 (0)20 7298 0600

USA - Northeast
21 West 46th Street, Suite 502,
New York, NY 10036
Tel: +1 646 396 0620

USA - West
2600 Network Blvd. Ste. 260
Frisco, TX 75034
Tel: +1 888 320 7372

Contact:
For inquiries about this report please email contact.us@theinstantgroup.com

Instant
RETHINKING WORKSPACE