REDSEAL B2B RESEARCH

Research methodology

An online survey was conducted by Atomik Research, on behalf of RedSeal, among 502 Senior IT professionals from the UK (up to CISO and CIO level). The research fieldwork took place on 19th-27th June, 2019. Atomik Research is an independent creative market research agency that employs MRS-certified researchers and abides to MRS code.

Breach activity

- 81% of UK businesses have suffered a cybersecurity breach in the last 12 months
- 39% said they only report the *large* breaches to their customers
- The impact on their companies after the breach was:
    - A third of UK Businesses (33%) said they lost customers
    - Over a third (35%) took cybersecurity more seriously
    - 34% said they suffered a damaged reputation
    - 31% said they had to hire new members to their IT team
    - Over a fifth (23%) lost revenue
- Following a breach it took 30% of those surveyed up to half an hour to get business back to normal and it took 25% a couple of hours.
- 40% of Senior IT Pros stat their business doesn't have a response plan in place to inform customers of a security breach.

Reporting a breach

- Almost 1 in 10 (7%) of Senior IT Pros still don't report incidents to Information Commissioner's Office
- Of those that do report to the ICO, the average amount of incidents they *have* reported is 5 incidents.

www.atomikresearch.co.uk
(T): 0207099 1010
(F): 020 7099 1010
tim.furdui@4media-group.com

19 Hayward Place
London

EC1R 0EH

- 33% of respondents said that they either don't have a cyber-incident plan or haven't test the one they have in place
- 26% are reporting *only* the major breaches to their CEO

CEO's impact on business and cyber risk

- One out of 10 (11%) said that decisions or actions made by their CEO or management meant that the business' cybersecurity has been at risk
- Three quarters (75%) think that their CEOs should pay more attention to cybersecurity in the future.
- Almost three quarters (74%) said that their customers' information has been put at risk because of a cyberattack
- Only 29% provide a daily cybercrime report to their CEO
- 14% of CEOs in UK business still haven't had cybersecurity training
- 54% of Senior IT Pros have a cyberplan specifically for their CEO but DON'T believe it's being followed

Senior IT Pros views on Smart Tech

- 95% say they are concerned that home smart devices could be hacked
- Only 62% are fully aware of the smart tech that their CEO is using in the home
- 48% of Senior IT Pros believe that the Government doesn't offer enough specific cybersecurity guidance and support to UK business

Brexit and Cybersecurity

- Almost three quarters (73%) of respondents said that the uncertainty around Brexit worries cybersecurity professionals on their team.
- 87% said that they find it difficult to attract skilled cybersecurity professionals to work at their business and that there is a real skill gap at their company.

www.atomikresearch.co.uk
(T): 0207099 1010
(F): 020 7099 1010
tim.furdui@4media-group.com

19 Hayward Place
London

EC1R 0EH

- When asked if Brexit will make it easier or harder to attract skilled cybersecurity professionals to their business 95% said it would be harder and 1% said it would be easier

Cyber Insurance

- Over three-fourths (77%) say their company has cyber insurance in place and 84% say that they believe having cyber insurance is valuable and/or necessary

---

Demographic data

Seniority

- More c-level executives report lost customers (38% vs 27% director) and damaged reputation (38% vs 28%) due to a cybersecurity breach. Directors reported lost revenue (28% vs 19% c-level), increased IT budget (34% vs 24% c-executive), taking cybersecurity more seriously (35% vs 31% c-level) and hired new IT team members (31% vs 26% c-level).
- More directors said it took within half an hour (39% vs 18% c-level) to get back to business after a breach while c-level executives said it took a couple of hours (41% vs 13% director).
- Directors said they had 5 breaches that their company had reported to the ICO and c-level executives said they had 6 breaches that their company reported.
- 72% of directors are tasked with reporting every breach to the CEO versus 64% of c-level executives who do the same.
- The majority (55%) of c-level executives meet with their senior team to discuss cybersecurity weekly while the majority (60%) of directors meet with their senior team monthly.
- 68% of c-level executives say they are fully aware of every single piece of technology in their CEO has in their home while 57% of directors say the same.

---

www.atomikresearch.co.uk
(T): 0207099 1010
(F): 020 7099 1010
tim.furdui@4media-group.com

19 Hayward Place
London

EC1R 0EH

Business Size

- Larger businesses were more likely to communicate a breach than smaller companies. 85% of companies with 1,001 employees or more said they reported all breaches versus companies with 51-150 employees, 34% said they reported all breaches.
- Larger companies lost more customers as a result of cybersecurity breaches 38% of companies with 1,001 employees reported a loss. 48% of companies with 1,001 employees also said they hired new IT team members and took cybersecurity more seriously more so than smaller companies.
- The smallest company group (51-150 employees) reported more breaches to their CEO. 86% of people that work at those companies said they reported every single breach.
- The largest bracket of employees said that their management has made actions that have meant that the business cybersecurity has been at risk, 17% said that their management had done this more than any other bracket.
- More people who work for 51-150 employee companies said that their CEO had received cybersecurity training 94% said their CEO had received the training.
- Smaller companies seem to be more worried about Brexit, 82% of people who work for companies with 51-150 employees said that the uncertainty around Brexit worried professionals on their team.

Revenue

- Companies with revenue of £300,000 or more per month experiences the lease amount of cyber security breaches in the last 12 months, 73% saying they have experiences them versus 86% of companies that make £50,000 - £149,999.
- 30% of companies that make £50,000 - £149,999 didn't report all of their security breaches to their customers but only the large breaches. 89% of companies that make £300,000 or more reported all of their breaches to their customers.

www.atomikresearch.co.uk
(T): 0207099 1010
(F): 020 7099 1010
tim.furdui@4media-group.com

19 Hayward Place
London

EC1R 0EH

- The companies with the smallest revenue (£50,000 - £149,999) and the companies with the largest revenue (£300,000 or more) both hired new IT team members (33% for the smallest and 51% for the largest) and took cybersecurity more seriously (25% for the smallest and 56% for the largest).
- 64% of people who work for a company with the smallest revenue (£50,000 - £149,999) said that their company does not have a plan in place to inform customers of a security breach vs 86% the company with the largest revenue (£300,000 or more) said that their does.

www.atomikresearch.co.uk
(T): 0207099 1010
(F): 020 7099 1010
tim.furdui@4media-group.com

19 Hayward Place
London

EC1R 0EH