Stanton house

## HOW DO CISOS CONVINCE EXECUTIVES THIS EQUATION ADDS UP?

# REMOTE WORKING + REDUCED REAL ESTATE COSTS = MORE CYBER SECURITY BUDGET

### Covid-19 business ‘winners’ and ‘losers’

There have been some clear business ‘winners’ and ‘losers’ as a result of Covid-19. Enforced social distancing has meant that industries such as hospitality and airlines were suddenly confronted with a crippling halt in customer demand - resulting in revenues which went through the floor. On the flipside, online retailers experienced the opposite and often struggled to keep up with, and capitalize on, the increased demand for online consumer goods and services.

| ‘Winners’ Camp | ‘Losers’ Camp |
|---|---|
| Online Retailers | Airlines |
| Remote Device Providers | Hospitality & Lodging |
| Business Architects | Entertainment / Events |
| Consulting Firms | Advertising & Media |
| Cybersecurity | Commercial Property |
| Cyber Criminals | Small Businesses |

No matter which Covid-19 ‘winners’ or ‘losers’ camp a business falls into however, it’s fair to say that the world of work has changed forever as we enter a new era of remote working. There are a multitude of evolving implications for business leaders to think about now and this includes the need to increase their Information and Cyber Security capability.

But as employers realize the many opportunities and challenges afforded by remote working, how high on the priority list is investment in Information and Cyber Security?

## Employers realize the benefits of remote working

Over the past few months, business leaders have had their eyes opened to the many benefits of remote working and are considering the significant cost savings that can be achieved with reduced real estate needs.

If you consider the floor space some large corporates take in the expensive high-rise buildings for example, these cost savings can amount to millions.

Leadership teams across the world, in organizations both large and small, are now debating how much of their workforce will continue working remotely in the long-term and are modelling different scenarios with reduced office space.

*“…crowded corporate offices with thousands of employees may be a thing of the past.”* **Jes Staley, Barclays CEO**

Just a few of the companies that have already announced intent to expand work-from-home include Morgan Stanley, Barclays, Thomson Reuters, Vodaphone, HSBC, Facebook and Unilever.

*“We’ve proven we can operate with no footprint….I see a future where part of every week, certainly part of every month, a lot of our employees will be at home.”* **James Gorman, Morgan Stanley, CEO**

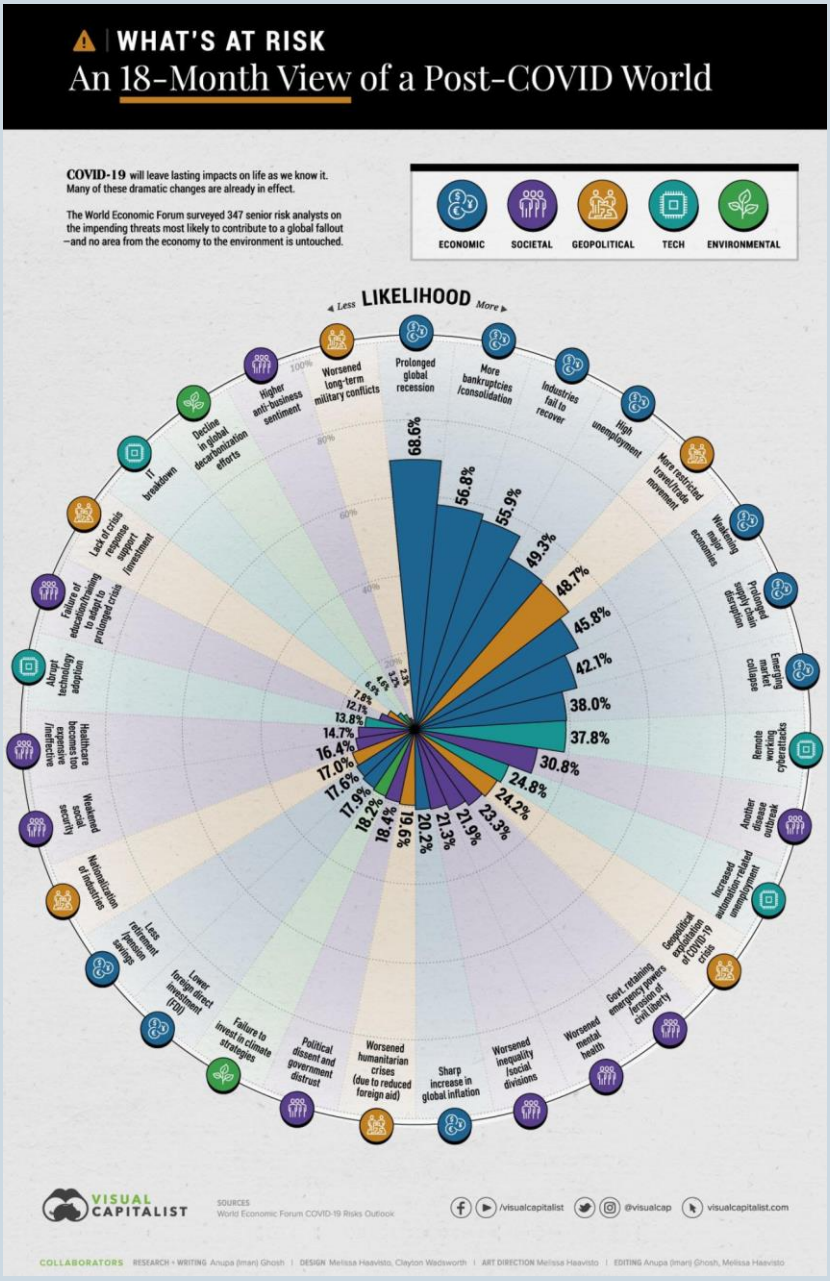
This commitment to expand remote working it is not just to save costs on office space. Most of the business leaders we speak to tell us they have experienced increased productivity, better collaboration and teamwork, increased employee engagement and a significant reduction in absenteeism - dispelling the many concerns and misconceptions to homeworking pre-Covid-19.

## ***Now*** **is the time for CISOs to secure investment**

Subsequently, executives are discussing what increased remote working and reduced real estate costs mean for investment and budgets for their different business functions going forward – including of course, Information and Cyber Security.

So, now more than ever CISOs need to ensure that they have a voice in these discussions and a seat at the board table.

According to the World Economic Forum's research on Covid-19 related risks, after economic and geopolitical risks, the **top** technical risk is cyberattacks on remote workers.




*Now* is the time for CISOs to shine a light on the inevitability of cyberattack, obtain buy-in from senior management, set best practice for secure remote working and influence key investment decisions (with regards to technology and talent) before it's too late.

But what does the canny CISO need to do to succeed in these endeavors? How is remote working impacting on security measures? What are the practical techniques needed to influence C-Suite executives to invest in something *intangible* and prevent something that hasn't happened…*yet*?

INSIGHTS

# How can CISOs influence budgeting decisions?

To get ‘real’ insight into this topic, we asked Senior Technology Leader, Dan Crisp to share the lessons he has learned and the techniques he has found most valuable in convincing key stakeholders to invest.

Many decision makers overestimate their company's cybersecurity defenses – ‘no news is good news’ and they may not be enthusiastic about allocating more budget to protect themselves.

*“One of the biggest barriers experts in our line of work find is convincing executives that doing nothing allows cybercriminals to gain advantage and potentially is putting the company at peril.”* **Dan Crisp, Senior Technology Leader**

According to Dan, there are several strategies which can be used to get past organizational resistance and convince decision makers to invest in Information and Cyber Security:

1. **Reframe success metrics - what worked before is no longer effective**

*“It is an arms race, what used to work doesn’t work six to twelve months later, you’ve constantly got to be thinking about upping your game and getting that across to non-technical people is essential. For want of a better analogy – executives need to understand that they can’t simply buy the car and then continue drive it for a decade - without servicing it - just because they don’t want to spend further money or buy a new one.”* **Dan Crisp, Senior Technology Leader**

Use problem statements to help push back on the status quo and facilitate conversations as to why what you’ve always done is no longer good enough. Here is an example:

***“Our information security management system requires reassessment and transformation to ensure continued effective protection for our clients and the company.”***

## 2. Benchmark with peers to challenge assumptions about the adequacy of cybersecurity investments

*"For example, when the Travelex breach occurred in London other currency exchange companies wanted to make sure it didn't happen to them. There were questions like – what was Travelex's Cyber Security footprint? What was their approach to risk management? How did it compare to their own company and therefore, how likely was this to happen to them?"* **Dan Crisp, Senior Technology Leader**

## 3. Follow the organisational expectations

- ✓ Use provided expected financial templates
- ✓ Work with finance in advance to ensure your budget can withstand challenge
- ✓ Use storytelling to illustrate the risk

*"Although it's important that you have done your homework, laid out a clear budget and you speak the language of finance – you want your conversations to be risk based- not dollars and cents based."* **Dan Crisp, Senior Technology Leader**

## 4. Refine your presentation approach

- ✓ Keep the focus on the risk to the organisation (operational, reputational, regulatory, litigation, etc.)
- ✓ Present in non-technical language
- ✓ Use storytelling to illustrate the risk
- ✓ Create a sense of urgency. Inaction is dangerous.
- ✓ Leave a strong document trail leading to the person(s) who grant budget
- ✓ Always provide a follow-up email regardless of the meeting outcome

*"You want to leave a strong document trail, and I call that the smoking gun, where it's been explained in layperson's terms and is abundantly clear to the budget granter – this is what's at stake"* **Dan Crisp, Senior Technology Leader**

## 5. Use the three-slide technique

- ✓ Problem statement
- ✓ Risk storytelling
- ✓ Solution with costing

*"The discovery of the three-slide technique is a defining moment in my career. When I was working for a bank, we had a Big 4 consultancy firm provided us with a 40-slide presentation deck, which we spent quite a bit of money on. We were to use these slides to present our justifications to the board for asking for exponentially more money. The CISO I worked with at the time said she didn't want to use them. She only wanted three slides. One explaining what the problem was. The second was to be the scary slide – explaining what would happen if they didn't address the problem. The third was the solution and cost. It was so powerful and effective that we got the funding we asked for. I have gone back and used this technique, incrementally, for projects and programme fund raising with great success"* **Dan Crisp, Senior Technology Leader**

## 6. Use narratives to illustrate the risk of inaction

*"I have found the use of narratives incredibly powerful. We used to call those the scary slides i.e. here's an example of something that has happened recently and here's why it might happen to you."* **Dan Crisp, Senior Technology Leader**

- ✓ News headlines *cause* decision makers to take action — even if it's short lived
- ✓ Storytelling activates sensory centers in the brain that make people relate to the story on a personal level — it places them *inside* of the story
- ✓ Storytelling is extremely powerful when it comes to marketing and other forms of communication

"*Use storytelling to demonstrate the risk, create a sense of urgency and leave them with the impression that you have laid this at their feet, with all of the risks and consequences outlined and now the decision is in their hands. "* **Dan Crisp, Senior Technology Leader**
*"You almost want to worm into a person's thinking so that they wake up in the middle of the night thinking about what you've laid at their feet. You want them thinking - what if we have a cyber-attack and I'm the budget granter who said no? That said, it's important to use storytelling to convey the drama for you- you want to portray yourself as the calm and collected person who has the plan"* **Dan Crisp, Senior Technology Leader**
*"A helpful the trick for me with the storytelling is to make them as scared as you are and no more. If you're stretching your own fear, it's going to be transparent."* ***CISO Advisor***

**Remember…you are competing for finite resources and budget. The best storytelling wins the day *and* the funding.**

So, while funds are in motion and rich savings are being made from reduced real estate costs it is imperative that Information and Cyber Security leaders have a plan to get the investment they need diverted to their new normal. There is a clear window of opportunity right now, to get the resources needed to ensure that there is continued Cyber Security hygiene.

## About Dan Crisp

Dan Crisp is the founder of Digital risk Insight, a technology risk strategic advisory consultancy. He began his career as a technology merger & acquisitions analyst at Citi. Subsequently, he led the technology risk, cyber risk, and Basel programs for JP Morgan Chase in the US. Dan went on to serve as Chief Operations Officer for Barclays Global Information Security in London. In this role, he was responsible for the technology due-diligence, uplift and technical integration of bank acquisitions in the US, Singapore, Johannesburg, Moscow, Madrid and Paris. During that time, he led the development of predictive quantitative operational risk models that inform and drive information technology investment decisions and ROI.

DIGITAL RISK INSIGHT

Prior to launching Digital Risk Insight, Dan served as the CISO and Chief Technology Risk Officer for BNY Mellon with technology risk, cybersecurity and data privacy oversight responsibility at BNY Mellon Corporation and its affiliates and subsidiaries. While there, he led the innovation, development and deployment of a global technology risk regulatory controls and analytics system for technology and privacy risk. Dan led the team that won the corporate innovation competition with their product proposal for a global cyber catastrophe bond reinsurance underwriting framework.

Since founding Digital Risk Insight, Dan led the creation and inception of the Financial Sector Cyber Collaboration Centre for the United Kingdom. He also introduced a Cloud Computing Controls Framework that has been adopted the world's largest cloud providers. In his current role, Dan provides cyber advisory services to boards, executive committees, risk organizations and technology organizations. He is currently providing services to the manufacturing, retail, e-commerce, technology start-up, energy, finance, insurance, IT and public sectors.

Dan has served as a board member of the Internet Security Alliance, a Non-Executive Director for Huntswood, a charter member of the Cloud Security Alliance metrics group, and is a senior mentor at Level 39, Europe's largest FinTech accelerator and incubator. The Financial Times has been recognised Dan on multiple years as a top 100 global executive in their annual leadership listing.

He received his BS at the University of Memphis (USA), and SAPM at Stanford University (USA). He has also completed the Strategic Management Program at Cambridge University (UK).

SIA STAFFING INDUSTRY ANALYSTS 2023 Best Staffing Firms to Work For

Great Place To Work. Certified FEB 2023-FEB 2024 USA

## About us

Stanton House is an award-winning provider of specialist recruitment solutions. Since launching in 2010, we have grown to over 50 employees and established offices in the US and the UK, having developed a customer-focused proposition that has laid the foundations for consistent success.

From our established office in Chicago, we deliver permanent and contract recruitment solutions to innovative organizations across North America looking to boost their Cybersecurity functions.

Whether you are looking to gain commercial advantage or concerned about the reputational risks of ineffective Cybersecurity, we can provide a solution that will support your strategic objectives.

We also support pre-IPO Cybersecurity Vendors looking to scale their organization with an all-encompassing talent solution. Our recruitment process is driven by expert teams, each committed to one specific function:

- **Cybersecurity**
- **Go-to-Market (GTM)**
- **Product & Engineering**
- **People & Finance**

With a deep commitment to the Cybersecurity sector, we offer tailored solutions, leveraging our expertise to serve clients' unique needs. By staying focused and true to our strengths, we ensure top-notch service delivery to foster long-lasting partnerships.