

INFORMATION SECURITY
**STARTS
HERE**

Managing remote workplace risks with ISO 27001



Lloyd's
Register



Almost all organizations have now been through a rapid and perhaps unexpected shift to widespread remote working. Even for those that were well prepared, the information security threat landscape has undeniably changed.

As remote working becomes an increasingly long term and strategic consideration - managing the associated risks will be a crucial, ongoing task that is central to protecting information and sensitive data.

Here, our panel of experts discuss the changing threat landscape, key actions you could consider and the important role that ISO 27001 certification plays in mitigating emerging risks.

The panelists...



Joyce van Luijn-Bonneveld

Sr. Lead Auditor, Information & Cyber Security
Lloyd's Register

Joyce is an experienced IT auditor and IT infrastructure project and change manager. She has been active in the business world for over 30 years as an IT line manager, project manager, and trainer/coach, and has several years of managerial experience.



Stuart Wright

Global Head of Compliance and Risk
Nettitude - A Lloyd's Register Company

Stuart has more than 17 years' experience in IT, and over 11 years' experience in the information security and consultancy sector. He has worked extensively across many different sectors, including retail, and local and central Government, Finance, and Healthcare.



Paul Raines

Chief Information Security Officer
United Nations Development Programme

In his capacity as Chief Information Security Officer, Paul is responsible for managing the cybersecurity and disaster recovery planning for the organization's 177 locations around the world. His unit is the first and only United Nations unit to be both ISO 9001, ISO 20000 and ISO 27001 certified.

Key takeaway 1 :

The changing threat landscape

Stuart: “Many of the threats that we’re seeing aren’t really new threats. Things like the use of home networks and home Wi-Fi, they’re not new; they’ve always been there. The difference is that with many more employees working remotely, the risk is greatly increased.

We certainly see more organizations prepared to allow their employees to use their own devices for work-related tasks - in many cases it’s necessary to keep the business going. We don’t own those devices as organizations, we can’t control the security of them, and we can’t make sure they’re patched and have antivirus and all the things they should. This lack of control introduces many more risks.

One risk that’s perhaps not being talked about as much is the disconnected workforce and the idea that when you take employees away from the office there’s a higher chance that they won’t report things that they would normally. This could include concerns, things they’ve done, links they’ve clicked on, and other incidents. This means we might not know when something’s potentially gone wrong and therefore, we can’t respond to it as quickly as we would have liked to.”



When you take employees away from the office there’s a higher chance that they won’t report things that they would normally.”

Stuart Wright

Global Head of Compliance and Risk, Nettitude - A Lloyd’s Register Company



Regardless of whether they have malicious intentions - friends, family and visitors could all find themselves in the vicinity of potentially unsecured devices and sensitive information.”

Joyce van Luijn-Bonneveld

Sr. Lead Auditor, Information & Cyber Security
Lloyd’s Register

Joyce: “Nowadays, we’re living in a digital era. Whether we’re booking a hotel room or ordering and purchasing personal items, it generates lots of data, which is stored in the cloud. There is a huge amount of information for hackers to exploit. This applies both to large organizations as well as individuals - and you - working remotely. Even with large companies that have implemented safety measures to prevent data breaches, there are plenty of examples of cyberattacks where data has been compromised.

As remote working becomes more widespread, and potentially permanent, opportunities for would-be attackers will grow and we’re likely to see more incidents. For example, employees may not have adequate and safe settings on their devices. Unauthorized access could also become an issue. Regardless of whether they have malicious intentions - friends, family and visitors could all find themselves in the vicinity of potentially unsecured devices and sensitive information.



Lloyd’s
Register

NETTITUDE
A LLOYD’S REGISTER COMPANY

Key takeaway 2 :

Awareness, behaviour and actions to protect your workplace

Joyce: “All organizations, regardless of whether they plan to work remotely long-term, must take steps to educate their remote workforce about the risks and the actions that they can take to stay secure. Examples could include how to spot phishing attacks and how to make a strong password.

Organizations should consider providing secure IT equipment to remote workers. They should also discourage them from taking sensitive documents to their homes and develop a set of policies and requirements that govern remote working.

Stuart: “Our users have access to data by design. They have access to a lot of data because they need it to do their jobs. This level of access makes it much harder to detect something that’s malicious because they have legitimate access to it in the first place through user credentials and permissions.

Criminals will target and value user credentials because by using stolen passwords, they can bypass a lot of our technical security controls. When they do that—when they have these credentials—they can appear as though they are that legitimate user which, again, makes it difficult for us to detect what’s happening and to respond to it. This reinforces something that most people recognize: that educating our employees is a crucial part of how we protect against these threats.”



All organizations, regardless of whether they plan to work remotely long-term, must take steps to educate their remote workforce about the risks and the actions that they can take to stay secure.”

Joyce van Luijn-Bonneveld
Sr. Lead Auditor, Information
& Cyber Security, Lloyd's Register

Joyce: “The loss of IT security and controls is a threat that’s often overlooked when working remotely. For example, an employee may not have proper safety settings on their devices. This could be because the company didn’t think about it or the employee uses their own equipment such as laptops or routers with standard passwords they didn’t change.

Sometimes there’s no antivirus or antimalware on the device, and critical updates don’t take place. In a different vein, the use of a virtual private network (VPN) to connect to the company isn’t always available, multi-factor authentication isn’t enforced, and other, unauthorized people such as employees’ family and friends could gain access—innocently or maliciously—to sensitive information.

It’s important to consider whether employees are paying enough attention and are aware of the risks regarding working at home. People should work on their own company or work computer and not share it with family members. They should change the passwords of their home routers and Wi-Fi and not use the standard, default ones provided because these are easily compromised. Instead, they should use unique passwords and not use them privately on websites like Amazon. Employees should also not leave their computer open and unlocked when away from it nor leave out any papers or confidential company data on their desk.”

Key takeaway 2 :

Awareness, behaviour and actions to protect your workplace

Stuart: “ISO 27001 can help you understand and mitigate the new risks that you might face with rapid change. It ensures that any changes you do make are made in a secure way with the right level of oversight and approval so that you’re not introducing new risks as a result.

There are many ways that you can make ISO 27001 work for you in the current climate, especially in areas like change and incident management, mobile devices and teleworking, assessing risk, carrying out audits, and monitoring security processes and controls.

Overall, a good Information Security Management System (ISMS) should support the objectives of the business; it’s there to help you stay secure. If you implement your ISMS well, it becomes how you do things, rather than an afterthought. It’s a highly effective method of managing risk even in the face of a truly unexpected event such as the recent pandemic.”



If you implement your ISMS well, it becomes how you do things, rather than an afterthought. It’s a highly effective method of managing risk even in the face of a truly unexpected event such as the recent pandemic.”

Stuart Wright

Global Head of Compliance and Risk
Nettitude - A Lloyd's Register Company



The ISO 27001 standard is a holistic set of controls which can be practically applied to mitigate the risks of working remotely.”

Joyce van Luijn-Bonneveld

Sr. Lead Auditor, Information & Cyber Security, Lloyd's Register

Joyce: “The ISO 27001 standard is a holistic set of controls which can be practically applied to mitigate the risks of working remotely.

In relation to remote working, some controls stand out. For example, the A.11 physical and environmental security control also applies to the remote workplace, and A.17 (business continuity) specifically addresses continuity of working remotely.

You could map the risks, especially for working away from company sites, and draw a comparison with some of the ISO 27001 security controls to create guidelines for remote working. These could include guidance around how and where to destroy paperwork, the use of company and personal devices, and network accessibility, amongst other things. You can then conduct internal audits and checks to review the effectiveness of these controls.”



Lloyd's
Register

NETTITUDE
A LLOYD'S REGISTER COMPANY

Key takeaway 3 :

ISO 27001 in practice: The United Nations Development Programme (UNDP)



My colleagues often ask me how I sleep at night with the challenges of the role I hold. Really, they're asking 'What have you done to demonstrate due diligence in protecting the reputation, finances and productivity of this organization from cyber threats.'

Paul Raines

Chief Information Security Officer
United Nations Development
Programme

Paul: "My colleagues often ask me how I sleep at night with the challenges of the role I hold. Really, they're asking 'What have you done to demonstrate due diligence in protecting the reputation, finances and productivity of this organization from cyber threats'.

We became certified to ISO 27001 in 2011. Prior to that, we had a major cyber breach that was widely reported and highly embarrassing for our organization.

As it turned out, we didn't lose much money, but we had the world's media following us and reporting the results of the breach, so it became a reputational issue for the organization. As a result, we immediately set forth in getting ISO 27001 certified. We also added ISO 9001 because that helped us to keep a customer focus, and ISO 20000 a little later on which covered IT service management. Since 2011 and securing these three certifications, we've had zero major cyber incidents that come close to what we previously experienced."

Paul: "By implementing management systems that comply with these ISO standards, you gain the confidence of management, your stakeholders, and your clients. If I could say one thing, it would be that cybersecurity is like oxygen. When you've got it, you don't think about it, but if you lose it, you can't think of anything else.

I think one of the things that ISO 27001 does for you is that it puts a record into your organization in terms of processes. In our organization, for example, we had a management review every three months and we were looking at how effective our security controls were.

If we saw a slippage or if a certain type of incident was occurring more often, say, for example, phishing incidents, then we would look at that and we would make decisions in order to address that and track it via future metrics to see if they were effective or not. I think it's that kind of rigour that comes with ISO 27001 that makes you a better security organization."



Cybersecurity is like oxygen. When you've got it, you don't think about it, but if you lose it, you can't think of anything else."

Paul Raines

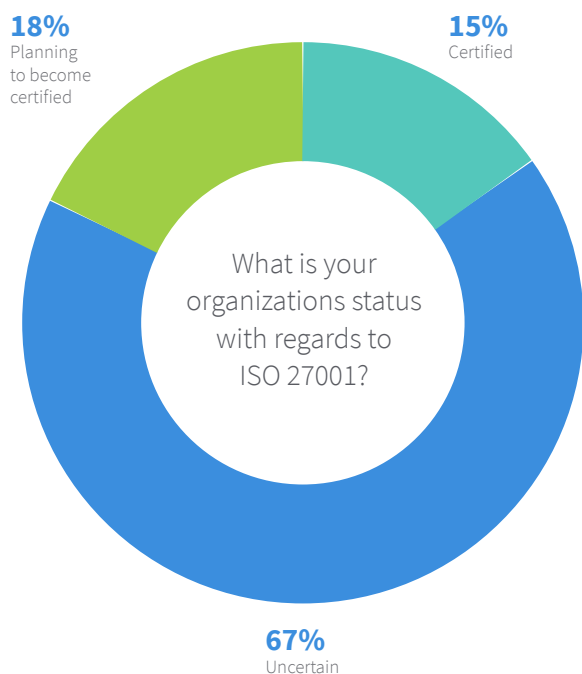
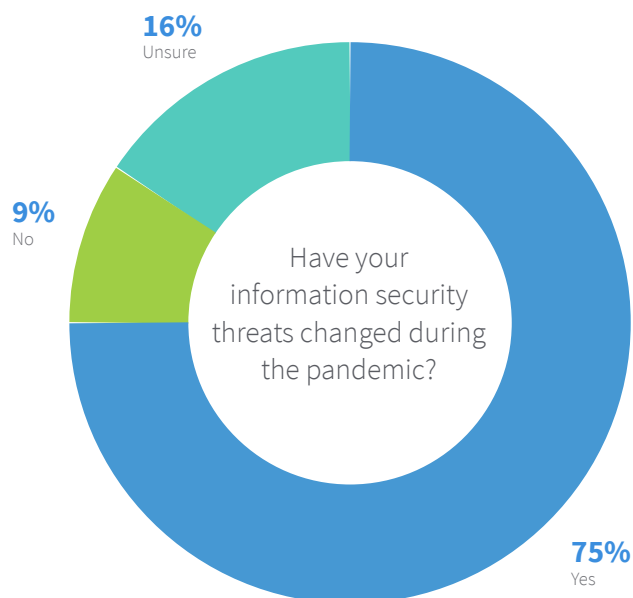
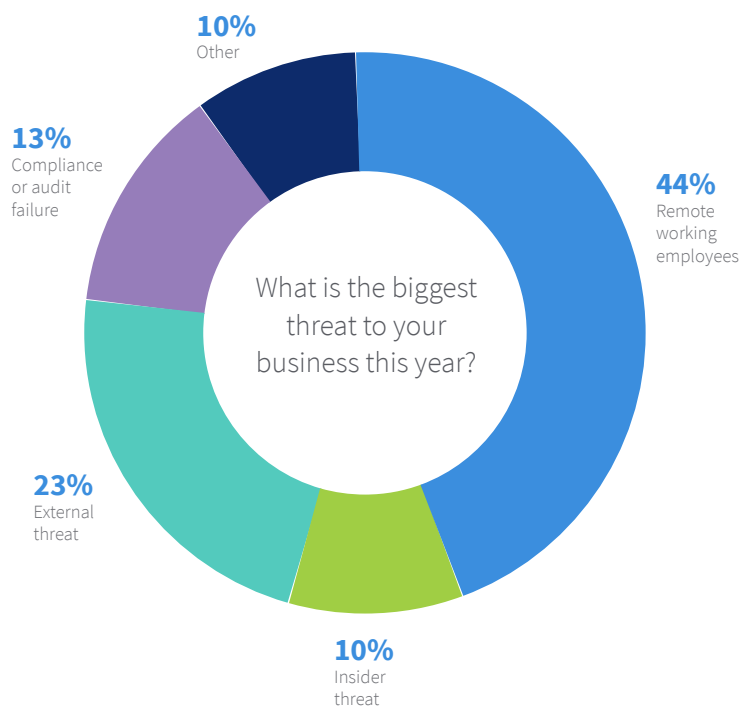
Chief Information Security Officer
United Nations Development
Programme



Lloyd's
Register

NETTITUDE
A LLOYD'S REGISTER COMPANY

Industry Views - what you had to say



Our ISO 27001 audit & training services

Our range of audit and training services are suitable for organizations of all sizes and locations and can help you make the most of the standards.

Ascend - Training from Lloyd's Register

LR's range of training services supports your organization throughout your journey to ISO 27001 certification. We understand that each and every one of us learns differently. That's why we provide our training courses in multiple different formats from face -to-face and Virtual Classroom options through to eLearning.

Our range of ISO 27001 training courses include:

- **Introduction to ISO 27001**
- **ISO 27001 Implementation**
- **ISO 27001 Internal Auditor, Lead Auditor, Lead Auditor Conversion**

Gap Analysis

This auditor-delivered activity offers the opportunity to focus on critical, high-risk or weak areas of your system in order to create a certifiable ISMS. Wherever you are in the certification process – the scope can be defined by you.

Certification

This is typically a two-stage process consisting of a system appraisal and an initial audit, the duration of which is dependent on the size and nature of your organization.

We can deliver your audit remotely through safe and secure platforms and applications. You'll receive the same high quality service with several added benefits such as flexibility, fast delivery and increased access to technical experts.

[Learn more here →](#)

Surveillance

Once we've approved your ISMS, we carry out regular surveillance visits to ensure the ongoing effectiveness of your system. This gives you, and your top management, the assurance that your ISMS is on track and continually improving.

Integrated management system assessment

If you're looking to combine your organization's ISMS with an existing management system (such as quality) you could benefit from a coordinated assessment and surveillance program.

Get in touch

Please visit **www.lr.org** for more information or **[email enquiries@lr.org](mailto:email.enquiries@lr.org)**



Lloyd's Register
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom



Lloyd's
Register

NETTITUDE
A LLOYD'S REGISTER COMPANY