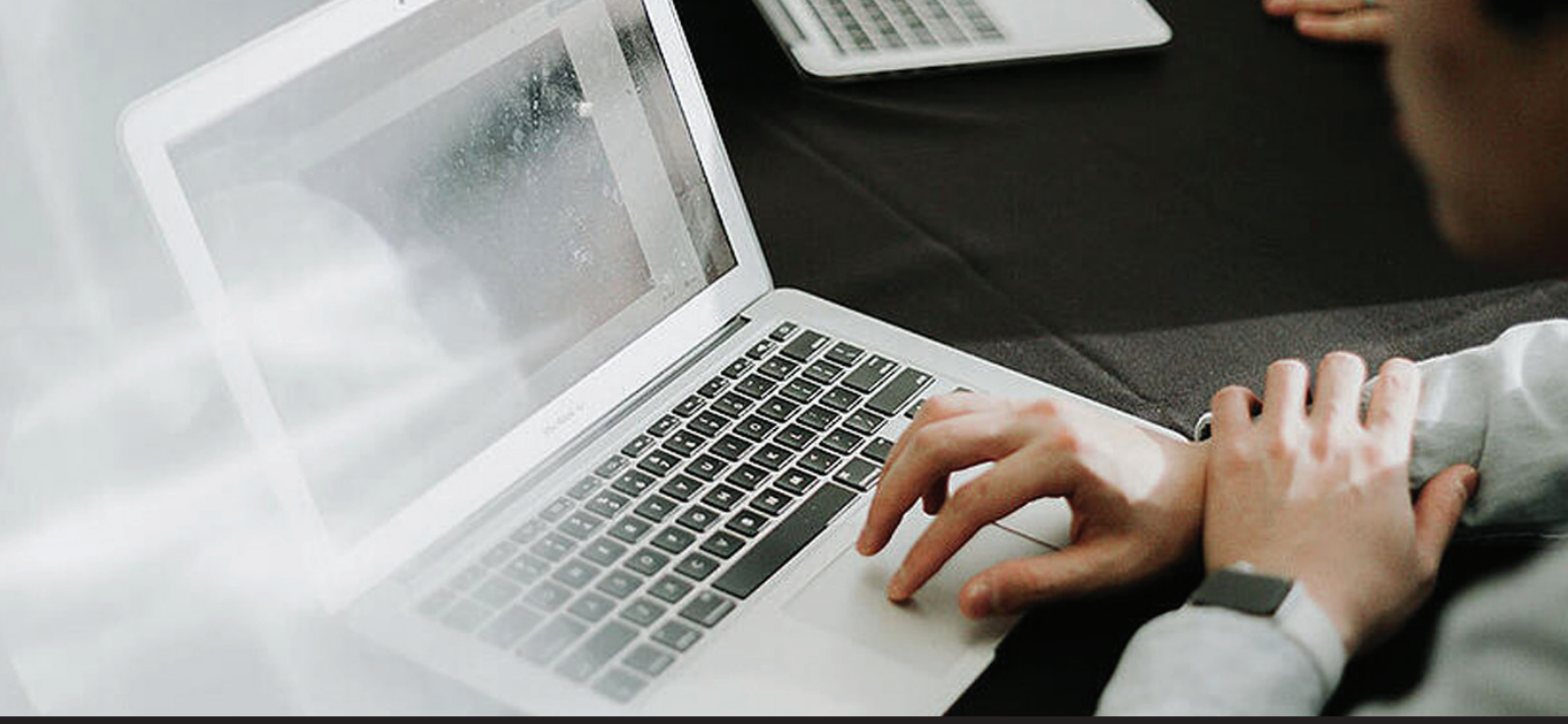

Data security is more than protecting digital assets - it's about protecting people and their right to privacy. Photo courtesy Zivver

How to prevent potentially life threatening human error data leaks

Data leaks seem to have become increasingly commonplace in recent year – or possibly we're just hearing more about them. In either case, such leaks are extremely serious for the safety and wellbeing of personnel across the globe. New, more effective working practises are needed to keep people safe.

Wouter Klinkhamer, CEO of Zivver

We are in the middle of a digital revolution, with growing volumes of confidential military information being digitized and shared electronically. In context with this shift, and the associated cyberwarfare threat, sometimes an incident occurs which casts new light on the importance of data security. For the 250 Afghan interpreters who fell victim to the recent UK Ministry of Defence (MoD) data leak, the impact was immeasurable.

The MoD fell into the same human-error shaped hole which thousands of organizations across the globe find themselves in, every year. For as long as humans are at the heart of workplace procedures – including military operations – errors will occur; making mistakes is, after all, human nature. It's the role of business leaders to support their teams and put the security of digital communications at the forefront ensuring that people have the right armoury in place when mistakes do happen.

The subject of great outrage, the MoD is currently under investigation for the Afghan interpreters' data exposure incident which, given the appropriate security practices, could have been prevented.

MoD email data leak – what happened?

On 21st September 2021, the BBC reported that the MoD had failed to protect personally identifiable information (PII) for 250 Afghan interpreters, just weeks after the Taliban captured Kabul and seized control of Afghanistan. This story highlights the devastating impact of an entirely avoidable security incident; the email addresses for 250 individuals were mistakenly copied into an email for all to see (the 'Cc' field used instead of 'Bcc').

As with the vast majority of data security incidents reported today (over 70 percent in the UK, according to the ICO), the MoD's PII leak is most likely due to basic human error. Thirty minutes after the initial email was sent, the MoD circulated a second email with the subject line "Urgent - Arap case contact," telling recipients to delete the previous email and warning "your email address may have been compromised."

With the incident under investigation and the story continuing to unfold, the MoD remains the subject of great criticism.

Data protection is people protection

By its very nature, the disastrous fallout of this particular data incident is rare. That said, it prompts an opportunity for forward-thinking leaders to review the way data is handled by staff across the organization - especially within sectors processing large amounts of confidential information, including the military. Those in charge of information security need to allocate time and resources to assess how sensitive data is being shared, and what support the organisation's workforce has to communicate securely. Incidents such as the MoD's email data leak often result from someone making a mistake. It is therefore necessary to focus on how to empower staff to be able to share information securely, with confidence and with ease to avoid a potentially damaging situation.

Protecting personally identifiable information goes beyond ensuring compliance; it is about respecting an individual's right to privacy.

Empower employees with the right digital tools

Cybersecurity goes beyond compulsory training and approved supplier lists. A 'security-first' lifestyle is one in which employees are empowered with the digital tools they require to perform their jobs as securely and efficiently as possible with minimal disruption.

While email remains a powerful tool, it leaves a lot to be desired in terms of security. Fortunately, technology is escalating

Wouter Klinkhamer, CEO of Zivver

to pick up where traditional email clients leave off. By automating manual tasks and providing users with real time support to apply appropriate data protection, the likelihood of an error occurring when emails are sent is dramatically reduced. A good analogy is the SatNav system, without which drivers make a lot of navigational mistakes. SatNav is not there to alert against making a bad choice – instead, it supports the user in making the right choices, all the time. That, to me, is the difference between risk mitigation and true enablement for people.

Another important consideration for military organizations is that most email delivery technologies still lack an effective revoke function. The reality is, in the instance of a data leak, employees are unable to act accordingly; they cannot determine when a message was accessed, by whom, or take the necessary steps to control the situation - all of which are issues likely experienced by the individuals involved in the MoD leak.

Whether accessing platforms on a private network or logging into a mobile banking application, two-factor authentication is a familiar practice to most of us. The same principle applies when sharing PII via email; every precaution must be taken to ensure only authorized individuals can access messages and attachments via the most user-friendly (and familiar) methods possible.

In addition, email encryption is vital in protecting sensitive data. Encrypting the connection between the sender and recipient's server prevents unauthorized users from intercepting communications whilst in transit. And, if an unauthorized user does gain access to encrypted files, they won't be able to read them.

To provide a 'reality check' on email encryption's current levels of usage; the most modern secure email standards guarantee that the mail servers (sending and receiving) are properly identified. But the adoption of these standards is lagging behind. Standard email encryption only goes so far as to 'see if' encryption is possible, but without guarantee that it is with the server of the intended recipient. And if the receiving server (or a man-in-the-middle hacker) denies encryption, the message is sent unsecured. In a growing number of use cases, authentication of the actual recipient is needed over authentication of their mail server. Traditional email technology lacks options to achieve mutual authentication without significant hassle for both sender and recipient. In the pursuit of true data protection enablement for staff, the provision of easy-to-use email encryption tools must be prioritized.

Turning best practice into standard practice

Maintaining data privacy should no longer be considered 'best practice' - it must be *standard practice*.

It is not enough to demand employees 'act securely,' utilize sub-standard technology, and complete compulsory training. Organizations are obliged to seek out secure communication platforms robust enough to fulfil privacy compliance, all the while aiding their people in safeguarding digital assets and therefore have the confidence to share content that matters.

A culmination of people, technology, and policy is needed to ensure truly effective data security in today's world.

Blaming people when technology and policy fails is a good way of turning your most valuable asset into your greatest security risk. Terms such as 'insider threat' and 'weakest link' are rife, and even 'human error' implies malicious intent within the workforce. In place of finger pointing, organizations must position employees as the data protectors they want them to be, taking the onus away from them and providing teams with the secure digital communication tools they require to succeed.

GMC