



Complying with Australian Data Protection Laws

ipswitch

A RECENT PONEMON STUDY ON THE IMPACT OF DATA BREACHES TO AUSTRALIAN BUSINESSES FOUND THAT STOCK VALUE DECLINED BY AN AVERAGE OF 5% AND CUSTOMER CHURN APPROACHED 7%.

THE SAME STUDY FOUND THAT 1/3 OF AUSTRALIAN CONSUMERS IMPACTED BY DATA BREACHES TERMINATED THE RELATIONSHIP WITH THE BREACHED ORGANIZATION.



New Breach Notification Requirements

In February of 2018, the Privacy Amendment (Notifiable Data Breaches) Bill 2016 takes effect. This law amends the data protection clauses of the Australian Privacy Act. At that point, all agencies and businesses regulated by the Privacy Act (those with more than \$3 million in annual turnover) will be further required to provide notice to the Australian Information Commissioner and affected persons of any data breaches which are likely to result in 'serious harm'.

While penalties for failure to comply with the Breach Notification amendment are as much as \$1.5 million, recent research by Ponemon Group shows that the total business impact of a data breach is much larger. Within days of a breach notification, businesses suffer an average 5% stock decline and a 7% customer churn. Fully one third of surveyed Australian consumers affected by a breach said they had terminated relations with the breached organization.

While Australian businesses regulated by the Privacy Act should assure they are prepared to fulfill the new notification requirements, the Ponemon study suggests the main focus should be on preventing data breaches in the first place.

With the external transfer of Personal Information (PI) now a core operational business process across a wide variety of industries, special consideration should be given to the security of file transfer systems. Legacy FTP servers are a particular risk as they are often targeted by cybercriminals as ideal Command & Control servers from which to execute Advanced Persistent Threats (APTs). In April of 2016, the US FBI dispatched an industry alert advising IT teams to assure the security of FTP servers as there was clear evidence of their role in a series of recent attacks.

IT organizations in industries such as retail, transportation, financial services, healthcare, entertainment, telecommunications and government as well as IT and business process outsourcers routinely collect, process and transmit PI. From a security perspective, data in transit is data at risk. IT teams must review their exposure to attack through the tools, technologies and processes they employ to externally share PI.

The Threat

Personal Information (PI) is typically defined as any data which by itself, or when combined with other data that the possessor can likely access, can be used to identify an individual. To a cybercriminal, access to PI makes organizations across a large number of industries lucrative targets for phishing, denial of service, ransomware and advanced persistent threat attacks.

Since 2013, publicly recorded data breaches have accounted for over 5.8 billion lost data records globally. The data lost includes passwords, health records, billing addresses and credit information.

While no industry that collects and stores PI is safe, sources such as the Breach Level Index report that 80% of the breaches occur in the technology, retail, financial and healthcare sectors. If your organization collects, stores, shares, processes or transmits Personal Information, you are a likely target for attack.

Much of the stolen data makes its way to a black market where prices vary by data type and age (how long ago it was stolen). Per record prices for passwords may be .10 to .20 USD whereas recently stolen credit cards can be worth from 25 to 40 USD.

The Enemy

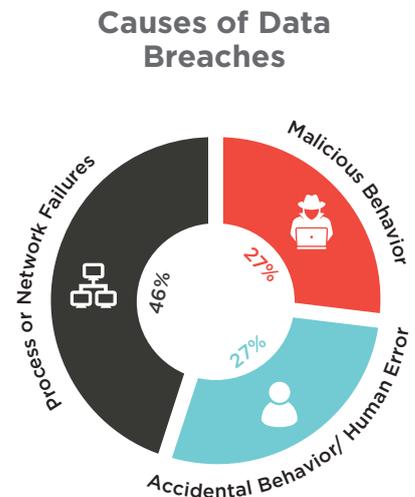
Who is responsible for these breaches? While the media would have us believe that the main culprits are nation states and cybercriminals, the truth is much less convenient. A recent Ipswitch survey of 255 IT professionals showed that only 27% of data breaches are the result of “Malicious Behavior”. An equal percentage are due to “Accidental Behavior or Human Error”. A staggering 46% of all data breaches were caused by “Process or Network Failures”. We’ve met the enemy and they are us.

The truth is that most data is lost because someone within the organization or within a partner organization does something they should not. Recent reports from Verizon and others also underscore the fact that while only 25% of all data breaches are originated by malicious insiders, unsuspecting insiders facilitate fully 75% of all data breaches.

For example, data may be transmitted through unencrypted email attachments or via web-based file share services. Additionally, your or a business partner’s employees may fall victim to a wide array of email or social media attacks.

Since 2013 , global **data breaches** have accounted for **5.8 billion lost data records.**

Source: Breach Level Index



In a recent email spoofing attack, employees of a healthcare organization were asked to respond with their EFSS user names and passwords – **60% complied.**



IT organizations should pay particular attention to the use of unsecured file-share technologies by employees and external partners such as email, unencrypted FTP and consumer-grade cloud services.



Your Risk Exposure

The first step in determining your organization's exposure to a potential data breach or non-compliance finding is to examine the systems and processes used to exchange data with external parties.

SCHEDULED FILE TRANSFER PROCESSES

Most likely your core file transfer processes, especially those involving PI, are already centralized to a small group of highly secured FTP servers. Hopefully, these use SFTP or FTPS which leverage SSH or SSL to assure encrypted transmission and authentication. Even SFTP/FTPS have limitations that expose you to an increased risk of security breaches and non-compliance.

Security/Compliance Risks of FTP

- › **Lack of Encryption:** If the server is not SFTP or FTPS capable, file transmissions are in plain text (unencrypted) and vulnerable to theft in transit through a number of easy to use technologies.
- › **Lack of Automation:** Repetitive manual file transfers leave organizations exposed to the risk of human error resulting in data loss. Scripts whose authors are no longer with the organization also pose a significant risk as they become outdated by process changes or updated security policies.
- › **Lack of Visibility:** FTP servers often lack the degree of visibility and logging required by auditors. The logs should be tamper-evident and track file transfer dates, receipt by the intended party, and whether or not the file was subsequently deleted.
- › **Lack of Scale:** Organizations often rely on IT to develop a collection of home grown scripts to automate their file transfer activities. As the needs of the organization grow, the scale and complexity of maintaining of these scripts become unwieldy and can introduce unanticipated security holes.

AD-HOC FILE TRANSFERS AND CLOUD-BASED TRANSMISSIONS

To maintain compliance with data protection regulations, your organization has to implement and monitor adherence to processes that assure the safe handling of PI. A particular vulnerability is the likelihood that an employee will transmit regulated data via an unsecured means such as an email attachment or via consumer-grade, cloud-based file share mechanisms.



Security/Compliance Risks of Email and Cloud-Based File Share

- › **Encryption:** Files are not likely to be encrypted during transfer. This would be a clear violation of most data protection regulations.
- › **Distribution:** There is no guarantee that transmitted data is only received by the intended recipient.
- › **Data Life:** Files are not deleted and data may continue to be exposed months after the initial exchange. A healthcare provider was fined two million USD for leaving unencrypted data exposed to the public internet for two weeks.
- › **Compliance in the Cloud:** Even when cloud-based file shares are advertised as ‘compliant’ the transmitting company is usually held responsible for assuring data security before, during and after the transmission.

File Transfer Security Controls

While the specifics of personal information protection regulations vary country to country, there are a core set of best-practice security controls that can help assure compliant file transfers. The ISO/IEC 27001 international standard, has been widely adopted across governments and industry sectors as it defines many of these best practices. The table below highlights the seven best-practice controls that are the most pertinent to external file transfer operations.

Security Requirement	ISO 27001 ref.	File Transfer Control
1. Compliance	A.18	Automation
2. Communications Security	A.13	Control & Visibility
3. Information Security Policies	A.5	Information Security
4. Access Control	A.9	Authentication
5. Cryptography	A.10	Cryptography
6. Physical & Environmental Security	A.11	Secure Architecture
7. Business Continuity Security	A.17	Failover

1

AUTOMATION

Commonly used file transfer workflows should be automated to mitigate against the introduction of human error that might result in data loss. Your file transfer tools should support functions such as automatic forwarding, error correction, and confirmation of receipt for all data transfers.

2

CONTROL AND VISIBILITY

Control and visibility of transfer activities are important security requirements and essential for validating compliance. Your tools should enable central visibility, control and prior authorization of all file transfers. Logs should be kept in a tamper-evident database to assure the integrity of audit trails.

3

INFORMATION SECURITY

Your technology, tools or processes should ensure file integrity checks, data deletion after receipt, and non-repudiation (the sender and receiver are both authorized and authenticated to access the data). They should provide an automated audit trail that tracks integrity, delivery and authentication

4

AUTHENTICATION

Effective authentication of users and administrators is an essential control. Your file transfer systems should accommodate an array of access control mechanisms, including integration with central user directories, role-based access control and single sign-on as well as multi-factor authentication.

5

CRYPTOGRAPHY

Encryption algorithms have a limited shelf life. Compliance standards often do not allow the use of compromised systems. It is essential that your systems employ strong, state-of-the-art cryptographic mechanisms and enable secure selection, distribution and protection of encryption keys.

6

SECURE ARCHITECTURE

Your systems architecture should integrate with existing security infrastructures and applications. The systems should also either ensure that there is no unencrypted data within the DMZ or provide for DMZ termination of inbound requests for authentication and data transfer with a gateway proxy server.

7

FAILOVER

A key requirement of many data protection regulations is secure business continuity. This requirement is meant to safeguard the confidentiality, integrity and availability of file transfers, at all stages throughout any failures, disasters or outages. Automatic, secure failover is essential to ensure that file transfers are either successful or continuously restarted until complete.

Case Study

How Medibank
Secures Sensitive
Information to
Meet Health
Industry
Regulations

Ipswitch MOVEit®

Secure Managed File Transfer

MOVEit® lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations. The table below shows how MOVEit addresses each of the seven core best-practices for compliance with data protection regulations.

Security Requirement	MOVEit Control
Compliance	MOVEit helps ensure that file transfers are secured, data is protected at all times, and records of transfers are secured in tamper-proof audit trails for legally required periods prior to assured destruction.
Communications Security	MOVEit enables central visibility, control and prior authorization of all file transfers, as well as encryption, traceability and non-repudiation of transfers, including secure audit trails of significant events. MOVEit is architected to integrate with existing security infrastructure, policies, and applications.
Information Security Policies	MOVEit encrypts files at rest and in transit, provides non-repudiation and file integrity checks. Ipswitch provides email, web, mobile access and desktop clients which, when used with MOVEit provide compliant file transfer access to all users.
Access Control	MOVEit offers a choice of authentication mechanisms, including integrations with existing systems, and a rich set of features to support user access management, including blacklists and whitelists.
Cryptography	MOVEit employs strong cryptographic mechanisms and secure selection, distribution and protection of encryption and decryption keys, consistent with international legal and regulatory requirements.
Physical & Environmental Security	MOVEit provides flexibility in implementation to ensure adherence to local physical security requirements.
Business Continuity Security	MOVEit safeguards the confidentiality, integrity and availability of file transfers at all stages throughout any failures, disasters or outages. Ipswitch Failover can assure uninterrupted file transfer processing.

About Ipswitch

With over 1 million users from 42,000 companies managing more than 150,000 networks in 116 countries, Ipswitch designs and develops industry-leading software that enables the easy delivery of 24/7 performance and security across cloud, virtual and on-premise environments. IT teams worldwide rely on 25 years of innovation to optimize and secure business transactions, applications and infrastructure with Ipswitch MOVEit® secure file transfer, Ipswitch WhatsUp® Gold network monitoring and Ipswitch WS_FTP®. Available directly or through strategic alliances with leading IT vendors and the company's fast-growing global partner ecosystem, Ipswitch's wide portfolio improves application and network performance, monitors diverse IT environments and ensures secure exchange of data that meets PCI, HIPAA, GDPR and other industry and government data security and regulatory requirements.

The company has offices throughout the U.S., Europe, Asia and Latin America. For more information, visit <https://www.ipswitch.com/> or connect on [LinkedIn](#) and [Twitter](#). To learn about Ipswitch's strategic alliances or global network of partners, visit <https://www.ipswitch.com/partners>.

ipswitch

See how easy it is to ensure your file transfer system complies with data privacy laws.

[Request your 30-Day FREE TRIAL of Ipswitch MOVEit >](#)