Understanding where your ERP starts and stops

A Guide for CFOs

Avoid becoming the next Cybercrime Headline

A growing number of CFOs are confronted with shock, dismay and some embarrassment when, after the implementation or upgrade of their ERP system, they discover they have still been defrauded by sophisticated cybercriminals. At best these stories are shared in private settings, at worst they make headlines.

eftsure

Enterprise Resource Planning (ERP) is Essential...

but Not All Powerful

ERP systems provide busy CFOs with many benefits, but they also come with limitations. And, given their responsibilities around governance, it's essential that modern day CFOs are clear on these shortcomings.

Today's ERP systems align with the changing role of CFOs, providing them with a unified view of the company's financial and non-financial operations at any point of time and enabling them to become involved in a wider range of projects across the business.

Given the many benefits of ERP, it's probably no surprise that global research and advisory company Gartner reports that ERP software sales grew by 10.7% to US$31 billion in 2017. Despite global economic concerns such as Brexit and trade wars, Gartner says the ERP market remains buoyant and is expected to show at least mid to high single digit growth in 2018. And, according to market research firm Statista, the global cloud ERP market is expected to be worth US$28 billion by 2022.

That's good news for major ERP system suppliers such as SAP, Oracle, Sage, Workday, Infor, Microsoft, Tech One, Civica, MYOB or Xero.

But despite the hype from marketers, ERP is not panacea for all a CFO's woes. Now more than ever, CFOs need to be aware of its limitations.

$31 billion

ERP software sales grew by 10.7% to US$31 billion in 2017

Here are a few important ones to consider:

#1

ERP can’t do everything

Just like every busy CFO, ERP can’t do everything.

ERP solutions are modular and require modules to be added to address further areas of business.

As John Catarinich, CEO of cloud ERP solutions provider Agilyx Australia, says: “Typically, many applications need to be complemented by special best of breed products. For example, customer relationship management (CRM) systems are not usually delivered as part of an ERP system and are often bought as a best of breed product and then integrated with other products that we sell.”

Similarly, he says Agilyx Australia will add succession planning, talent management or staff engagement extensions to human capital management (HCM) platforms as these are not found in traditional ERP systems.

Agilyx

#2

Not all systems are the same

A look at the many reviews of ERP platforms shows that they vary widely in terms of what they address, the features they provide and how their modules integrate with others. Some aren't suitable for, say, small or very large businesses and different providers offer differing levels of support or pricing structures.

That's why Ted Needleman, writing in PCMag after **reviewing** a range of ERP solutions last year, advised CFOs to really do their homework before making choices.

Just like PCMag's review, one of the most recent comparisons, **Magic Quadrant for Cloud ERP for Product-Centric Midsize Enterprises**, conducted by Gartner in 2018, also reveals a wide range in the quality of solutions offered by providers.

"Disparity between the maturity of cloud offerings in HCM, finance and operational ERP reflects the increasing prevalence of postmodern ERP strategies in which traditional ERP suites are being deconstructed into more loosely coupled applications," Gartner notes in its report.

Writing in a recent **article** in CFO magazine, Nicolas Nicolaou, who as a CFO has been involved in numerous ERP systems implementations during his career, adds that it's very important to select the right technology platform for the needs of a particular business.

"Vendors will try to oversell on their solutions. You don't want to overpay for technology that has functionality you may not need or that's too complicated for a small business," he says.

Sometimes it's better to buy a less complex ERP solution and then buy further specialised software modules for other purposes like vendor management, CRM, succession planning, talent management or HCM.

CFO Magazine
Nicolas Nicolaou

#3

Too big to be included

Catarinich notes that some types of data cannot be fully integrated into ERP systems. Take asset management systems, for example.

"If the range of assets is very sophisticated and large, there will be in a separate platform, but the total value of those assets can still be measured in the ERP system," he says.

"The ERP system may consider these other systems sub-ledgers or sub-systems. It will take summary information from them and retain this within the main ERP platform."

#4

Legacies of complexities

For CFOs, Catarinich highlights several shortcomings when it comes to trying to capture billing information in ERP systems.

He notes that the inbound information for a billing system, which is the amount received from customers or a sales amount, finds its way into an ERP system very quickly and can easily be accounted for.

The difficulties, however, centre around the complexity of very large billing systems. This is because bank account numbers from suppliers change frequently and new clients are constantly added to the system. Plus, suppliers self-manage their bank account, payment and other details in some ERP systems.

In addition, many of those once vaulted work horses – legacy platforms – can't be swapped out because they are so customised or because they have a connection with customers' billing systems.

"Often billing systems are very old and/or extremely large-scale containing hundreds, if not millions, of rows of data associated with all their customers and which may not be replaced very easily," adds Catarinich.

All this means the billing records and data may also have to be kept separate to the ERP system.

#5

Security risks

Worse still are ERP systems' potential limitations when it comes to the efficacy and security of payments.

We know that data entry errors as simple as misspelling are common and virtually impossible to eliminate, and that this can result in duplicate vendor or customer accounts being created.

But a far bigger worry for any CFO is the threats of fraud and cybercrime.

Australian Bankers Association (ABA) payment files, for example, are text files and are therefore editable, exposing a business to the risk of fraud.

Plus, all IT systems, including ERP, are vulnerable to cybercrime, even if they have adopted security measures such as firewalls or the patching of servers.

This leaves them exposed to a host of different types of attacks, including distributed denial of service (DDos), ransomware, malware, phishing and business email compromise (BEC). And, no matter how hard an organisation works to combat them, the threats keep evolving and cybercriminals just keep getting better at what they do.

According to a new threat **research** report, cyber-attackers are exploiting ERP business-critical applications.

The research, conducted by risk management firm Digital Shadows and ERP cybersecurity and compliance firm Onapsis, shows a dramatic rise in cyberattacks on widely-used ERP applications such as SAP and Oracle — which currently have a combined 9,000 known security vulnerabilities.

The report also highlights an increase in attacks on these systems by nation-state actors, cybercriminals and hacktivists that include both hacking and DDoS attempts to compromise and disrupt the operations of these high-value assets.

This convergence of threats puts thousands of organisations and their crown jewels directly at risk of espionage, sabotage and financial fraud, the researchers say.

This report's findings were considered so critical that the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) issued an alert on the day the report was released warning of the risk of these ERP application attacks.

These findings illustrate how new technologies can be a double-edged sword. As Catarinich observes, because they make payments more efficient, these systems allow fraud to occur just as efficiently (if systems are not complemented by other measures).

"If one person supplies details, updates records and makes payments, without separation of those duties, fraud is actually very easy to perpetuate and very hard to detect," he says.

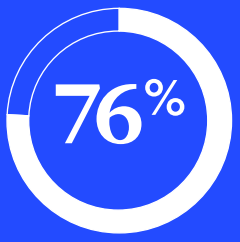
For CFOs, the guardians of the corporate purse strings, this is of great concern. Verizon's 2018 Data Breach Investigations Report, based on the analysis of thousands of real-world incidents, found that 76% of the breaches were financially motivated. And over a quarter (28%) of attacks involved insiders.

Closer to home, *PwC's 2018 Global Economic Crime & Fraud Survey: Australian Report* reveals that the majority of fraud and economic crime in Australia – 60% – was committed by someone close to the organisation, such as an employee, customer, supplier, consultant or agent.

Worryingly, the report notes that customer fraud is now the number one type of economic crime in Australia.

When it comes to external threats, PwC says cybercrime tops the list. In the past two years, almost half (43%) of the Australian organisations PwC surveyed said they had suffered a cyberattack. However, PWC believes the number is probably much higher and the problem is only likely to get worse.

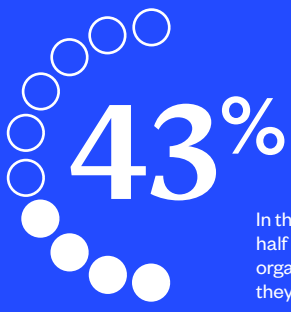
PwC notes that cybercrime thrives on the same kinds of technologies that organisations are using to drive growth. For example, while adopting cloud computing and the Internet of Things can lead to improved efficiencies and innovations, they also increase the number of 'attack surfaces' for cybercriminals to target.



financially motivated breaches

of attacks involved insiders

The majority of fraud and economic crime in Australia – 60% – was committed by someone close to the organisation.



In the past two years, almost half (43%) of the Australian organisations PwC surveyed said they had suffered a cyberattack

"This does not mean that organisations should retreat from technology. Instead, they need to design, build, test and deploy with cyber in mind," says PwC in its report.

A solution

Agilyx integrates eftsure into many of the ERP systems it curates for customers to help them identify and protect themselves against the risks and errors which can occur in the supplier payment process.

As with most limitations in the IT world, there's usually a solution. For Catarinich, it comes via eftsure.

To put it simply, eftsure assists by verifying supplier data and validating changes when they occur. It also helps to streamline the supplier onboarding process and ensure payee compliance.

"eftsure operates with our ERP system which means that when payment runs are selected or when payees are selected for payment, an automatic validation occurs to check up on various of criteria," says Catarinich.

"This could include whether those suppliers are being paid for the first time or if there's a different bank account or if the bank account is not identified at all."

"eftsure also checks whether an amount is larger than the last payment by various criteria – for example, by five or 10 times – and can determine whether changes in account details have been made, corrected and approved."

Catarinich says the use emails, text messages and twitter today has removed a level of human check points or hurdles that might have stopped fraud and cybercrime in the past. **"Interrupting that with other measures like eftsure, for example, is helpful,"** he says.

The eftsure solution does three things in concert to help protect organisations:

Payments Protection

eftsure matches payee names with BSB and account numbers, something that banks don't do. This ensures that the party you intend to pay, actually receives it. It is 'always on', does this in real time and delivers signals on your online banking screen or prior to ABA file upload. By way of simple signals, it alerts you to anomalies, and reduces the risk of fraud and error prior to your bank releasing your funds for payment. It also warns against out of range payments and duplicate payments.

Vendor Management

The first step to an error and fraud free vendor master file is discovering how healthy that file is. eftsure runs a comprehensive verification report on your vendor master file. This provides you with a risk and error scorecard and dashboard that shows the accuracy of your client data. This snapshot of a constantly changing database might surprise you. eftsure typically finds 25% anomalies in Vendor Master Files that require review across a number of categories including incorrect bank account numbers, invalid/deregistered companies, duplicate entries etc – many of which have the potential of resulting in payment issues.

eftsure's online portal allows suppliers' details to be onboarded to an organisation's vendor master file quicker and with less errors than legacy processes. It also ensures that the data is independently verified by eftsure. It also ensures that once on-boarded, accounts departments are notified of any changes to supplier data details in real time.

eftsure is a more efficient and effective way of managing data, and getting the data onboarded to the vendor master file correctly, quickly and without errors in the first place. It reduces time and the associated costs of dealing with the onboarding and maintenance of supplier by removing the burden of acquiring and capturing of accurate supplier data from the company's staff and ensuring only accurate, independently verified data is delivered to the customer's ERP.

Compliance

eftsure allows your organisation to constantly monitor critical information that assists you with new ATO legislation (such as The Taxable Payments Reporting System – TPRS), auditing and other compliance commitments including signalling the credit worthiness, ABN validity and GST Registration status of suppliers.

Regardless of what sector your business operates in, compliance is crucial and so too is efficient and effective payment reporting.

Enhance your ERP

ERP has changed the operational management of business and delivers myriad benefits to the C-suite, including the CFO. However, it has several often-overlooked limitations. Notably, its inability to protect a business and its finance function from rapidly evolving, increasingly external cyber threats.

In eftsure, there is a solution that enhances your ERP by adding a payments protection layer to ERP and financial controls. eftsure sits effortlessly alongside existing ERP packages and associated business processes and workflows or can be integrated into them.

Get in touch to find out how eftsure can help secure your payment system.

Ed Elliff

T: 1300 985 976
E: ede@eftsure.com.au
sales@eftsure.com.au