ERP Maestro Security, Governance, Risk and Compliance Insights Survey Summary

A report summarizing the results of the May 2018 Americas' SAP Users' Group Survey: ERP Maestro Security, Governance, Risk and Compliance Insights

Table of Contents

Introduction

Studies indicate that data breaches were up by 44.7 percent in 2017 and nearly $2 billion records containing personal and sensitive data were compromised. Enterprise resource planning (ERP) systems process huge amounts of transactional data and can be lucrative targets for such attacks. In fact, 77 percent of the world's transaction revenue touches an SAP system. Yet, many companies using SAP may overestimate the security of their SAP-based workload, and adoption of ERP security solutions is still low, despite the apparent need, risk and degree of concern about cybersecurity across the enterprise.

A May 2018 survey of IT, security and audit professionals using SAP conducted by Americas' SAP Users' Group (ASUG) and sponsored by ERP Maestro uncovered insights on:

- Some of the biggest challenges of internal security/compliance
- Which aspects of governance, risk and compliance (GRC) are viewed as the most difficult to automate
- How automation minimizes GRC challenges
- ERP migration to the cloud

This paper is a summary of the survey results and examines possible factors impacting the survey conclusions.

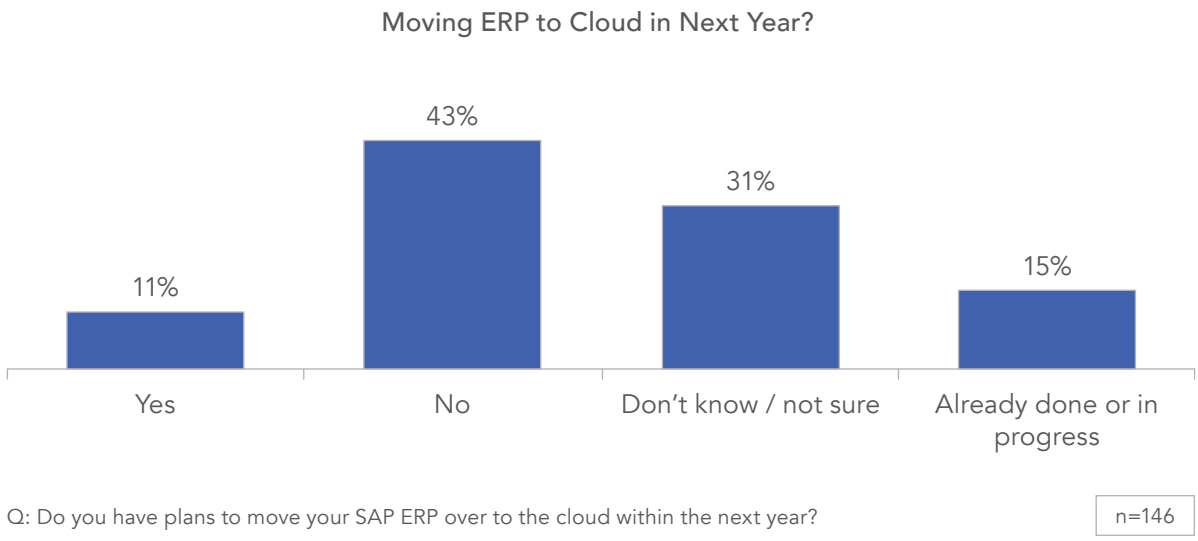
Survey Results

SAP Product Use

The survey included responses from both customers using SAP on-premise and those using SAP delivered as a cloud solution.

As noted in the survey results, SAP ECC is still the dominant core ERP used among ASUG members. While SAP HANA has been adopted by half of survey respondents, SAP S/4HANA still has lower penetration. Additionally, one in ten companies is planning an ERP migration to the cloud within the next year, bringing expected penetration to nearly 25 percent.

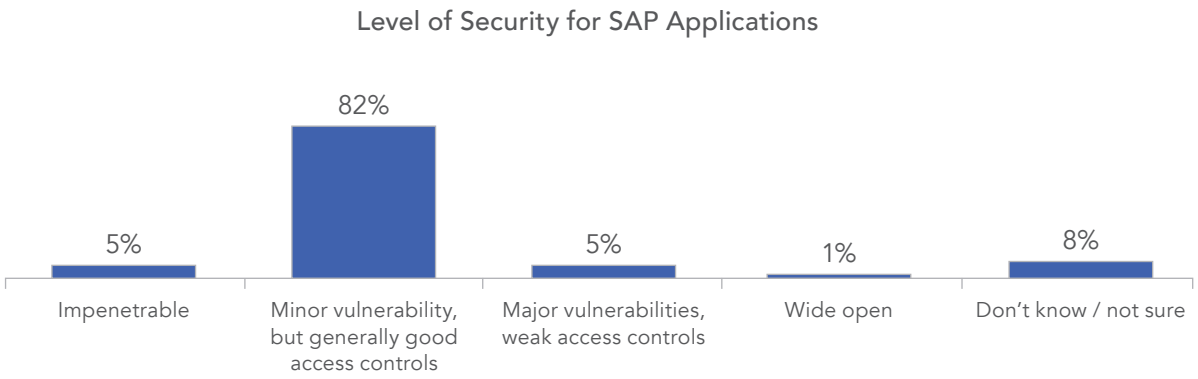
Many companies are holding back and continuing use of ERP on-premise, perhaps to take advantage of existing contracts or to wait for potential challenges (cloud security, implementation costs) to abate. According to ERP Maestro, as greater understanding of the safety and benefits of cloud technology and automated access controls increases, adoption rates should also rise.



Q: Do you have plans to move your SAP ERP over to the cloud within the next year? n=146

System Vulnerabilities to Attacks

As survey responses showed, a majority of the respondents, 82 percent, classify their systems as only having "minor vulnerabilities." Because, as a key insight of the report stated above, many companies using SAP may overestimate the security of their SAP-based workloads, they may rate their vulnerabilities lower overall. It is also possible that without automated tools, companies may lack the visibility into the number and scope of actual risks and vulnerabilities.



Level of Concern About Cybersecurity

By contrast to the vulnerability ratings, 50 percent or more of the respondents in four out of five of the role categories surveyed ranked their level of concern about security as very or extremely concerned highest on a scale of extremely concerned to not at all concerned.

The degree of concern does seem to indicate that there is at least a high level of awareness of the potential for breaches and related damages; however, it also suggests that there is a disconnect in perceived vulnerabilities as related to level of concern. It could further denote that respondents aren't completely confident in their monitoring and prevention strategies or tools even though they view their vulnerabilities as minimal.

	IT/SAP security	IT management (non-security)	IT analyst	Executive / management	Finance / business analyst
Extremely concerned	35%	11%	17%	17%	8%
Very concerned	45%	38%	39%	8%	42%
	80%	49%	56%	25%	50%
Somewhat concerned	10%	38%	31%	42%	25%
Not very concerned	5%	11%	11%	33%	17%
Not at all concerned	5%	3%	3%	0%	8%

Q: How concerned are you with the level of security around your SAP data and systems?

In respect to security and perceived vulnerabilities, the assumption is that most security threats stem from malicious outside hackers. Even though external breaches may cost companies hundreds of thousands of dollars, they may appear to be relatively easier to identify and fix with traditional security measures. Moreover, external threats have historically gotten the lion's share of attention. Insider threats, on the other hand, may remain largely unreported due to insufficient evidence or concerns about negative publicity or consequences. Strikingly, though, insider attacks are more pervasive with 75 percent of all cyberattacks being carried out by people within the organization. Most internal attacks are also accidental—the result of employees exposing sensitive data unwittingly, performing transactions accidentally or having their access compromised.

According to Ponemon Institute's 2017 Cost of Data Breach, the average total cost of data breach was $3.62 million. However, the cost of a data breach is not limited to affecting the bottom line alone. There are other serious repercussions that are set in motion when sensitive data gets compromised, namely the erosion of trust with customers, board members, investors, employees and the public that causes irrevocable damage to a business's reputation. Despite the detrimental effects of a breach, which include legal implications and regulatory fines, there is less concern among C-level executives, which could lead to complacency or failure to take preventative actions or put forth strategies to fortify sensitive information.

Role Level and Degree of Concern

Among the survey respondents, 25 percent of management and executives reported that they are very and extremely concerned about security. They are most optimistic about security in general, perhaps because they are not as directly involved in security work or responsible for it. The respondents most concerned, 80 percent, were predominantly IT, security and analyst employees or those with governance, risk and compliance (GRC) responsibility.

According to the ASUG survey report, dedicated security professionals understand the nuances of security and see it as a significant challenge. They likely have a more accurate assessment of their environment.

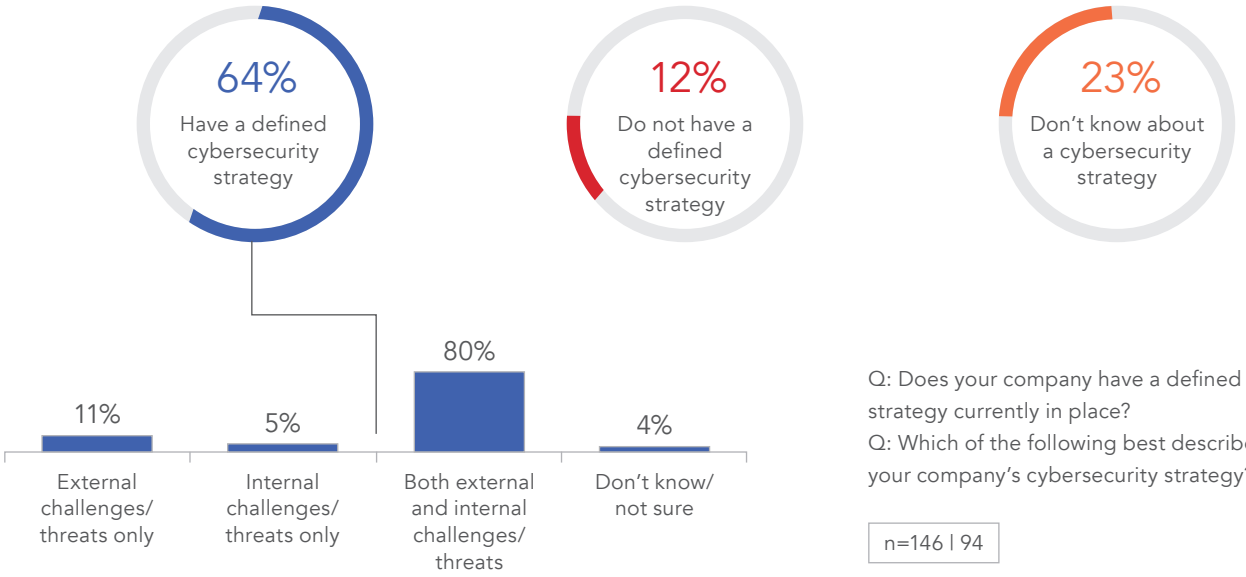
The lack of concern among executive-level employees may indicate that more education is needed among this cohort to help increase understanding of the potential risks and insider threats. Because senior-management employees are generally the ultimate decision makers on budgeting and spending for security tools, their knowledge deficiency could lead to not being fully protected against internal breaches or not approving the investment in better defense solutions.

50 percent or more of the respondents in four out of five of the role categories surveyed ranked their level of concern about security as very or extremely concerned

Correlation of Cybersecurity Strategy and Level of Concern

Survey participants were asked if their company has a defined cybersecurity strategy in place. Only two-thirds of respondents have a strategy. This supports the level of concern, particularly among IT/security staff.

ERP Maestro advises that a well-defined security strategy that includes easy-to-manage access control monitoring, Segregation of Duties (SOD) analysis, access reviews, remediation, user provisioning and de-provisioning and audit reporting can increase confidence in security safeguards and decrease concern.



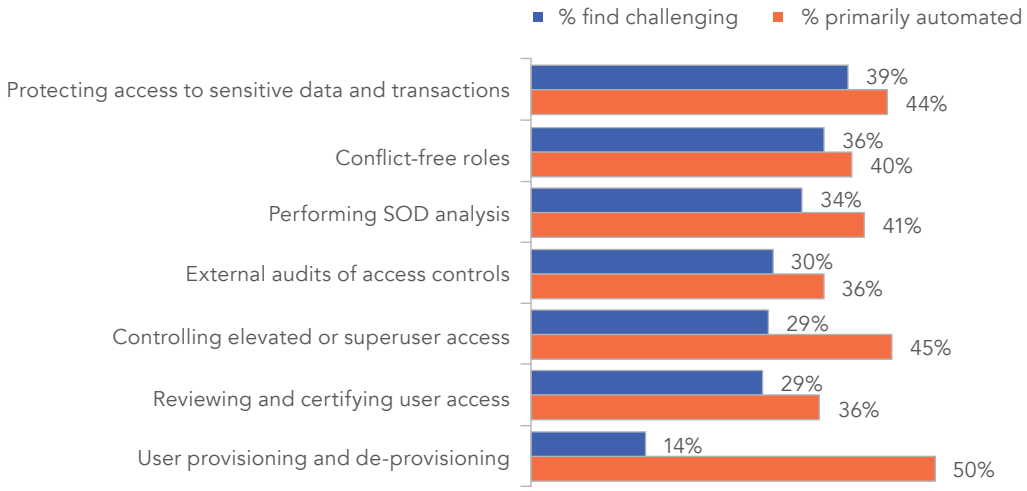
Q: Does your company have a defined cybersecurity strategy currently in place?
Q: Which of the following best describes the focus of your company's cybersecurity strategy?

n=146 | 94

Automation and GRC Challenges

The survey revealed that while there is not one particularly significant challenge reported within a company's GRC areas, the biggest opportunity for improvements is in data protection. Automation does minimize GRC challenges within core ERP systems, at least in part, according to survey key insights.

User provisioning and de-provisioning were reported as the most automated and least challenging GRC areas, while user access review is seen as the biggest challenge to automate and is automated the least. There is a moderate-to-high negative correlation between the degree of challenge and the level of automation within the ERP system. As automation decreases, in many cases the GRC area becomes more challenging.



Q: For each of the following security and compliance areas, how would you rate the level of challenge it presents for your company specific to your company's SAP environment?
Q: For each of the following security and compliance areas, which option best describes how you handle this process?

n=146

As ERP Maestro explains, the time- and cost-intensive nature of access reviews alone should encourage companies to automate the processes. The main ways a company analyzes and verifies internal controls for access controls, auditing and compliance is through access reviews. The reviews enable a business to detect over-provisioned accounts, catch identity access management exceptions and ultimately prevent insider threats.

Done manually, access reviews demand a lot of effort and require back-and-forth interactions between various stakeholders, increasing the hours and cost of performing review activities. They can also be rife with inaccuracies.
A typical review completed in this manner can take many weeks and generally involves the following steps:

"There is a moderate-to-high negative correlation between the degree of challenge and the level of automation within the ERP system. As automation decreases, in many cases the GRC area becomes more challenging."

It may take as long as two weeks, for instance, just to create a report and begin a review process, which involves sending the report to managers for review/approval/action. It can take much longer tracking and following up with managers who most likely will not complete the required review in the time requested. Add to that the total hours it takes for each manager to conclude a review. For some companies, this process may involve hundreds of managers, resulting in many weeks that could be used for more strategic initiatives.

Another issue with manual review processes is how the reports are presented to the business owners. Manual reports are pulled directly from the ERP system and use technical descriptions such as roles, groups, authorizations, tcodes, etc. Managers are required to approve user access to these roles. Often there is a risk of managers engaging in rubber-stamping. Rubber-stamping can easily occur for multiple reasons: 1) the review is tedious and the manager just wants to get it over with, 2) the manager doesn't understand what is being asked of them, doesn't understand the importance of performing the review, or doesn't understand technical jargon so rubber stamps to get it out of the way, or 3) because they can. There's no way to prevent this when spreadsheets are used. While providing access to wrong people may appear less harmless than taking away the access to an employee and inhibiting him/her from performing a critical task, in the long run it is an added risk to the business.

Automation can diminish the work, inaccuracies and overall cost of access reviews.

Moreover, the survey revealed that automation and a defined cybersecurity strategy are linked. Those with a defined strategy are significantly more likely to use automation in many of the GRC areas.

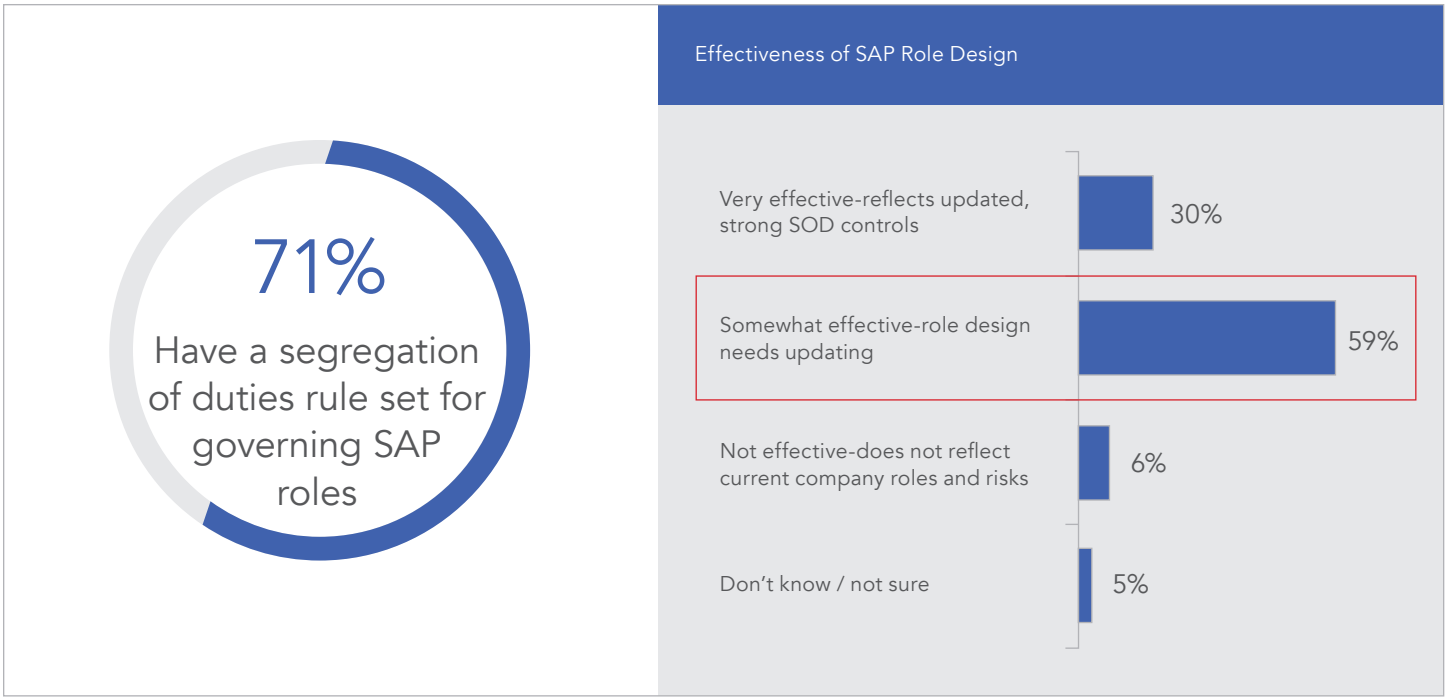
% who are fully or mostly automated within each area	Have cybersecurity strategy	No cybersecurity strategy	Don't know
Controlling elevated or superuser access	**52%**	28%	32%
Protecting access to sensitive data and transaction	48%	44%	32%
Performing SOD analysis	**47%**	28%	32%
User provisioning and de-provisioning	**56%**	44%	35%
Conflict-free roles	**44%**	33%	32%
External audits of access controls	38%	33%	32%
Reviewing and certifying user access	**41%**	17%	29%

Q: For each of the following security and compliance areas, which option best describes how you handle this process?
Q: Does your company have a defined cybersecurity strategy currently in place?

Segregation of Duties Insights

In the ASUG member survey, most companies confirmed they had a sound SOD rule set in place to govern SAP roles. However, a majority, 59 percent, of the respondents feel that roles currently reflected in the system need an overhaul.

"A majority, 59 percent, of the respondents feel that roles currently reflected in the system need an overhaul."



Q: Does your company have a segregation of duty (SOD) risk rule to govern SAP roles and access?
Q: In your opinion, how effective is the design of SAP user roles within the system?

n=146

Common SOD best practices and a sound cybersecurity strategy require the ongoing maintenance of roles in order to reduce the instances of insider attacks and secure the SAP environment.

Roles can be designed in multiple ways; two of the most common are job-based or task-based. When roles are designed around specific jobs, they continue to grow in parallel as jobs evolve, eventually leading to bloated roles.

Designing roles around tasks limits the duplication of access and allows for flexibility and scalability, thus lending to easy maintenance. Task-based role designs are more secure because they limit the access to only what the user needs to perform the job.

Awareness of Security Solutions

Participants in the survey were also asked about their experience with and awareness of security solution vendors. ERP Maestro topped the list with the greatest level of brand recognition, 62 percent, among SAP users surveyed.

ERP Maestro was the most recognized security solution vendor among survey respondents.

Conclusion

The first step towards securing a company's SAP system is understanding what the company's high-value assets are and prioritizing security measures to protect them. Real risk areas can be identified and defined using a good sensitive access rulebook that allows customization based on the specific business. The next step is having robust access controls that deliver visibility into risks and a platform that manages access and enables accurate and easy review and reporting.

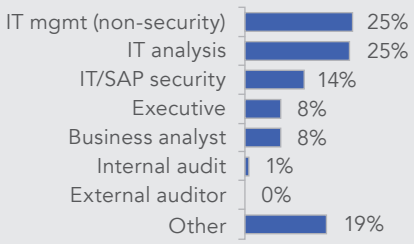
In today's complex ERP environments, companies should consider using sophisticated tools for access controls that can adapt to the constantly evolving risk factors and allow the businesses to grow without being bogged down by breaches. Equipping the risk management team with automated tools that can quickly analyze big data and provide easily digestible reports for both the business and the IT community within the organizations, can help educate and ensure the involvement of non-security staff in the risk management process.

As the survey results indicate, automation can minimize GRC challenges. When automation increases, challenges decrease. No industry is immune to cybersecurity risks, but "The biggest risk to any enterprise's security comes not from employee actions, but organizational inaction: the failure to act until after a breach occurs."

For more details about the ERP Maestro Security, Governance, Risk and Compliance Insights survey contact: marketing@erpmaestro.com

Survey Demographics

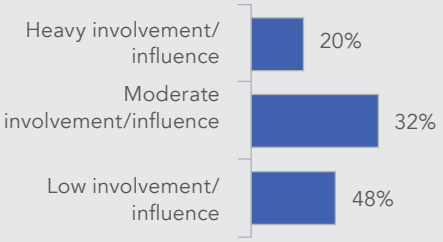
Job Title



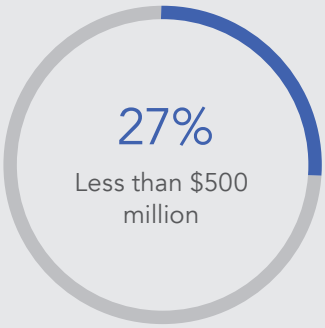
Industry

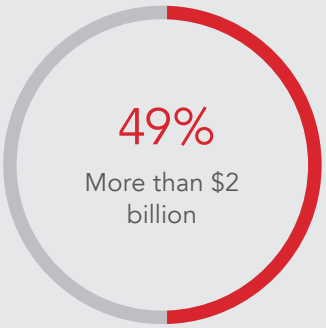
Public sector	14%
Technology/software	10%
Retail, medical/pharma	8%
Utilities	7%
Oil & Gas, CPG, auto	5%
Chemicals	4%
Aviation/aerospace	3%
Finance, entertainment	1%
Telecommunication	0%
Other	28%

Security Involvement



Annual Revenue





About ASUG

Founded in 1991 by four pioneers who understood the potential of SAP software, the Americas' SAP Users' Group (ASUG) today is the world's largest independent SAP user group with 2,400+ corporate members. ASUG's mission is to help our members maximize the value of their SAP investments. So no matter where you are on your SAP journey, ASUG is here to help you navigate every step of the way. Find membership information at https://www.asug.com/join

About ERP Maestro

ERP Maestro makes managing security incredibly easy with its automated controls for access, security and GRC. Used by seven of the world's top 10 audit firms, its cloud technology platform automates the monitoring, detection and prevention of internal cybersecurity risks, accelerates remediation and simplifies audits and compliance. Learn more at www.erpmaestro.com.

Sources

https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

https://www.sap.com/corporate/en/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html

ASUG May 2018 ERP Maestro Security Governance, Risk, and Compliance Insights

https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach- incidents/

https://www.ibm.com/account/reg/us-en/signup?formid=urx-15763

https://www.itgovernance.co.uk/blog/what-if-the-threat-comes-from-the-inside-77-of-privilege-misuse-caused-by-internal-actors/

https://www.sap.com/corporate/en/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.htm