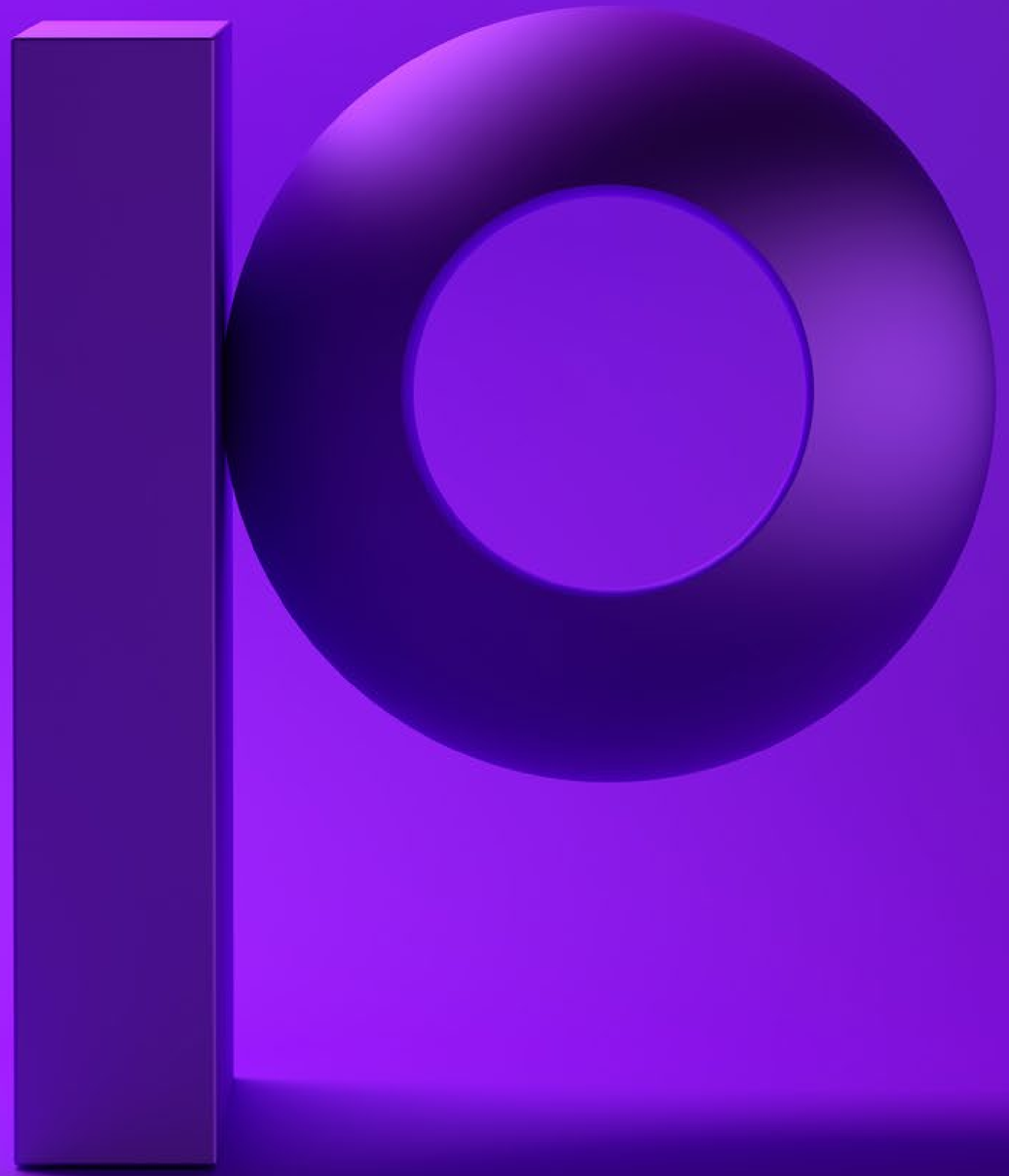
precisely

IBM i Security Insights for 2020

Key Data Points from Precisely's Annual IBM i Security Survey



Introduction

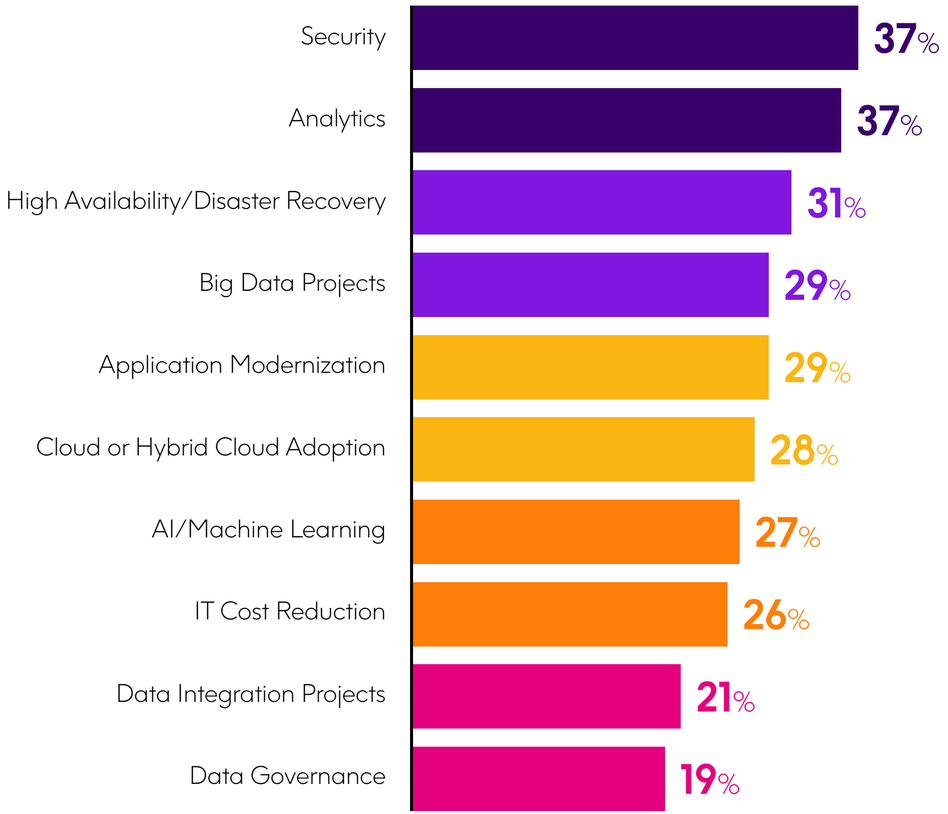
For the past three years, Precisely has annually surveyed IT professionals who are responsible for IBM i security at their company about their present and future security concerns for the IBM i platform. Our survey was conducted in late 2019, and as with previous years, covered numerous topics, such as technologies installed, procurements planned, compliance regulations followed, audits performed, breaches experienced, and more. These survey results provide a revealing look at the current state of IBM i security.

When respondents were asked to indicate their company's top five IT priorities for the coming year, security was the most-selected priority. This is the second year in a row that security was named the top IT priority of organizations. This is telling, given the growing array of security and compliance challenges that companies are facing, many of which we'll examine more closely in the coming pages.

Of the respondents to our survey:

- 48% have primar y responsibility for IBM i security, 52% share responsibility
- 78% work in companies of more than 100 employees, 57% work in companies with more than 500 employees
- 10% work for Healthcare companies, 10% for Financial Ser vices, 10% for Computer Ser vices, 9% for Banking

What are your organization's top five IT priorities for the coming year? (Select five)

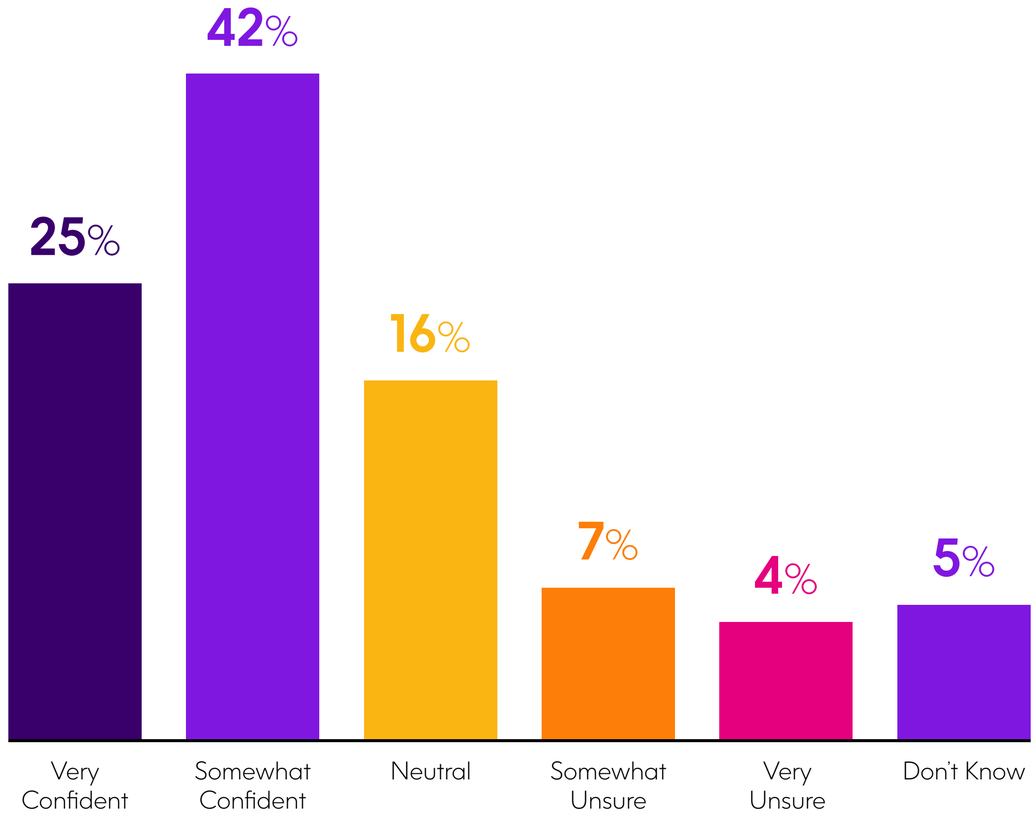


Note: the above chart only shows the top 10 choices – the actual sur vey question had many other options. In addition, because respondents were asked to select five choices, the figures don't total to 100%.

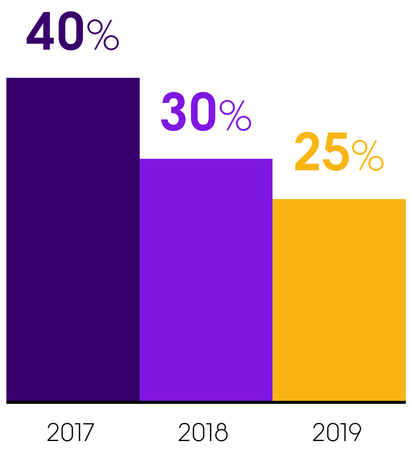
Another key metric from this year's survey is a noticeable drop in respondents' confidence in the ability of their IBM i security program to prevent a breach. This year only 25% of respondents said they were very confident, a significant drop from the 40% who reported the same level of confidence in 2017. In addition, those who have a low level of confidence (reported they were somewhat or very unsure of their confidence to prevent a breach) has risen noticeably from 0% in our 2017 survey to 11% this year. Our survey did show an additional 42% who indicated they were somewhat confident, but this is also a sizable drop from the 54% measured last year. This lowered confidence level may be what is driving security to the top of IT priorities.

This trend of dropping levels of security-confidence is corroborated by a **2019 survey conducted by Microsoft** on behalf of Marsh, one of the largest global-risk insurance companies. From 2017 to 2019, their survey showed a 100% increase in respondents who said they were not at all confident in their ability to understand, assess, and measure cyber threats, and a 63% increase in no-confidence votes when it came to the ability to mitigate or prevent cyberattacks.

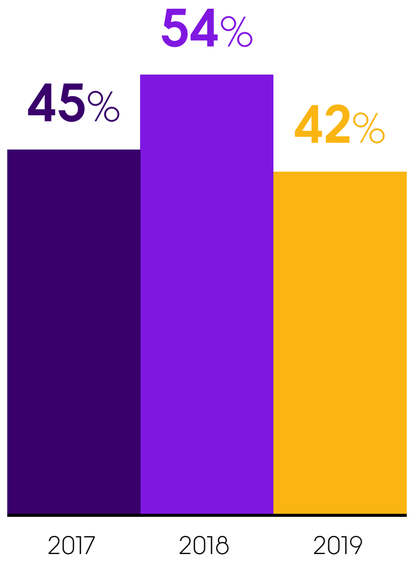
How confident are you in the ability of your IBM i security program to prevent data breaches today?



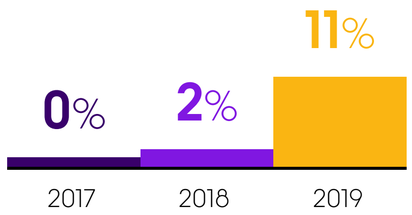
Year-over-year change in breach-prevention confidence levels



Very Confident



Somewhat Confident



Somewhat or Very Unconfident

Top Security Challenges

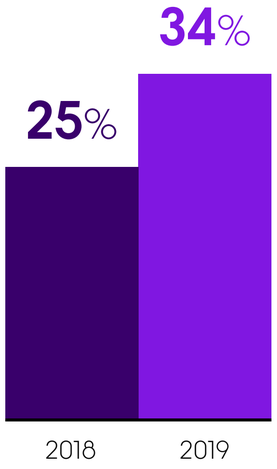
When respondents were asked to choose their top three security-related challenges from a list, the most selected included:

- **Complexity of regulations** — The most prevalent challenge cited this year was the growing complexity of regulations, with 34% choosing it as one of their top three challenges. This was a sizable increase from the 25% who selected this challenge last year. With compliance regulations impacting companies with greater frequency, it makes sense that this was selected as the top challenge by IBM i professionals. We'll talk more about the challenges associated with compliance regulations in the next section.

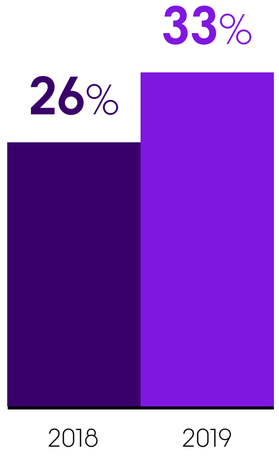
- **Data from other platforms** — Companies are increasingly contending with numerous security challenges when data from other platforms integrates with their IBM i infrastructure. This was made evident in various challenges selected by respondents. For instance, the adoption of cloud services was the second- most-selected challenge this year at 33%, up from 26% last year. This in turn was followed by the challenge of securing data that comes from new sources at 29%, which was up from 20% reported last year. This year 20% also specified the challenge of data becoming increasingly distributed.

- **Security training and expertise** — Additional numbers in this survey reflect the challenges of expanding security expertise among IT staff along with improving security awareness among users. The challenge of inadequate training for IT staff is up from 8% last year to 21% this year, and inadequate training for end-users has grown from 9% to 21%. The challenge of insufficient IT security staffing stayed roughly the same this year at 15%, which is still significant. It's likely these training and staffing challenges are worsened by the challenge of insufficient IT security budgets, which is up from 11% last year to 15% this year.

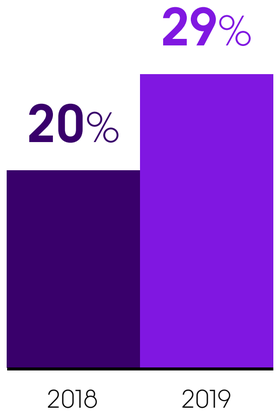
Year-over-year changes



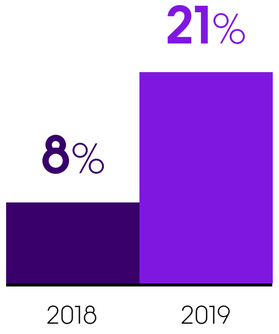
Growing Complexity of Regulations



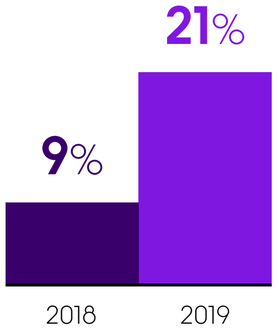
Adoption of Cloud Services



Securing Data from New Sources



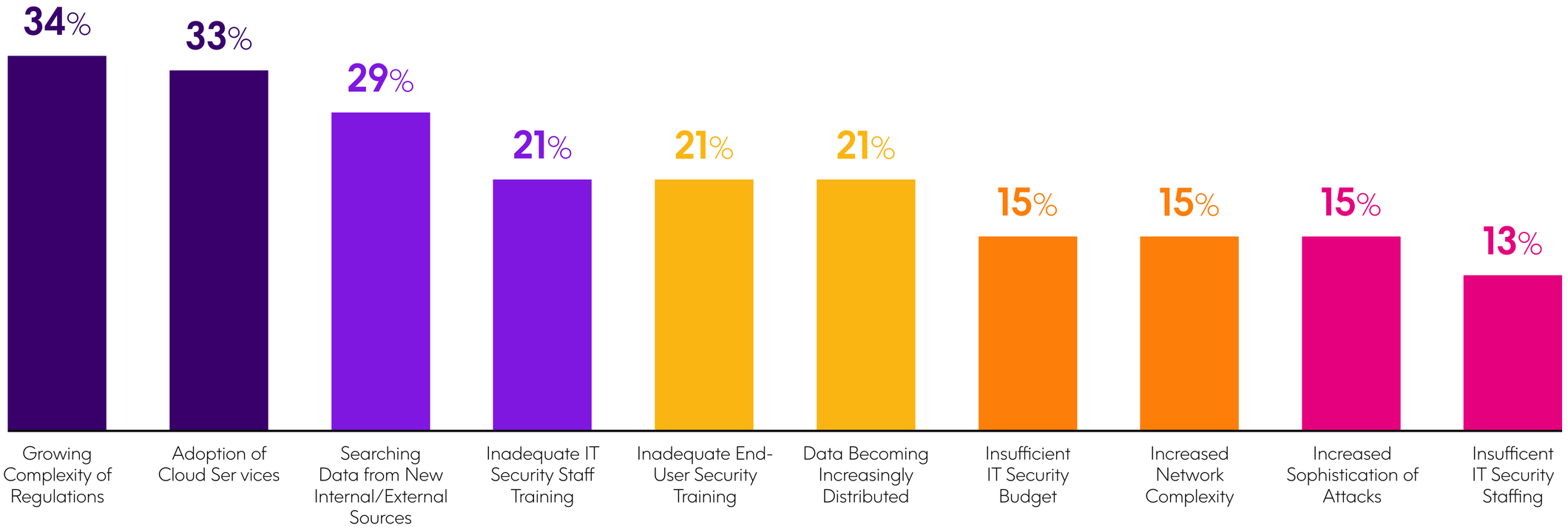
Inadequate Training for IT Staff



Inadequate Training for End Users

What are your organization's top three security-related challenges?

Choose three options.



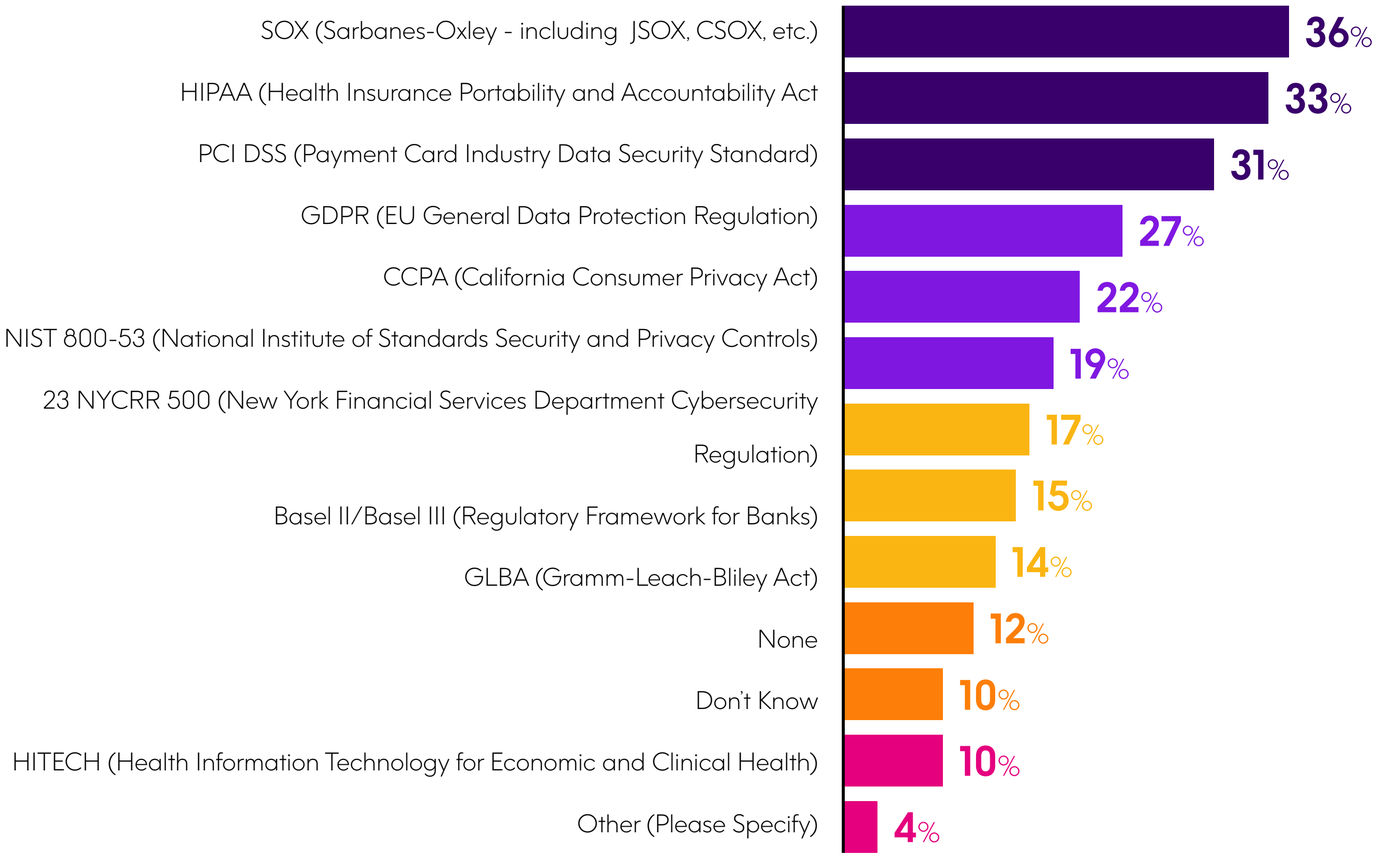
Note: because respondents were asked to select ten choices, the figures don't total to 100%.

Regulatory Requirements

With the steady increase in the number and scope of regulations, it is understandable that the most frequently selected security challenge in our sur vey was the complexity of regulations. In fact, 80% of our sur vey respondents said their company was required to comply with one or more regulations and nearly 90% of respondents reported having some type of sensitive data on their IBM i ser vers. When asked about the nature of this sensitive data, 48% of respondents cited corporate financial reports, 39% said they have business strategy information, and 38% have financial transaction records, all of which aligns with SOX being the regulation that affects the most companies in our sur vey. Right behind the prevalence of financial information on IBM i is sensitive data that relates to consumer or healthcare information.

What regulations must your organization adhere to?

Choose all that apply.

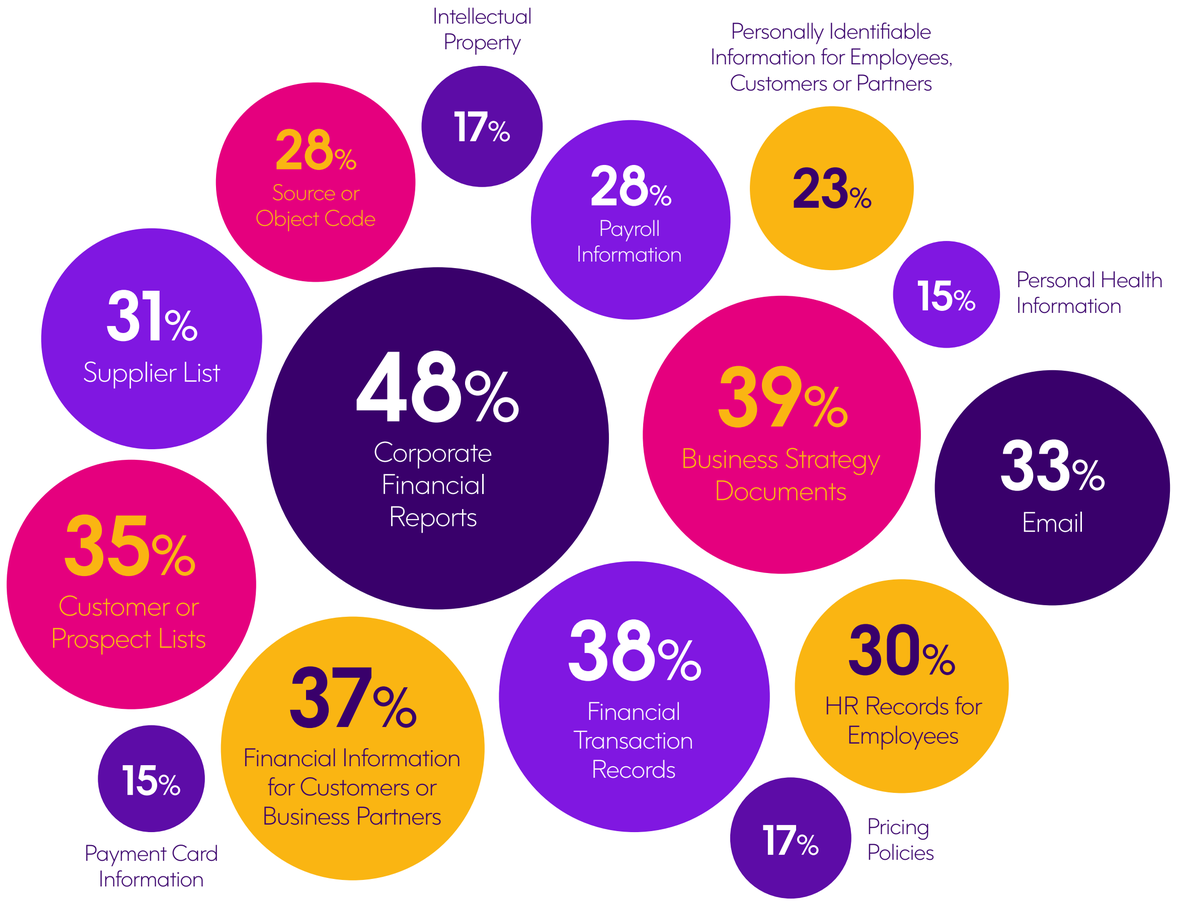


Note: Respondents were asked to "select all that apply;" therefore, figures don't total to 100%.

The challenge of dealing with regulations drives home the necessity of having regular access to IBM i security expertise—whether in-house or from third parties—as well as making ongoing efforts to improve auditing, access control, and activity-tracking and reporting capabilities. Recently enacted regulations like GDPR and CCPA mandate strong data privacy policies, driving the need for technologies that provide encryption and secure file transfer capabilities. In short, companies simply cannot be complacent as regulations will constantly change and new ones are certain to come along.

What type(s) of data reside on your IBM i systems?

Choose all that apply.



Note: Respondents were asked to "select all that apply;" therefore, figures don't total to 100%.

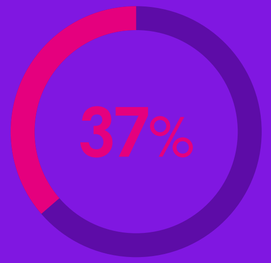
Security and Compliance Audits

Many compliance regulations require companies to perform periodic audits of their security procedures and technologies. 80% of our survey respondents say their company undergoes regulatory compliance audits at least once per year (an increase from the 70% cited last year), and 84% report passing their compliance audits when they do occur. Respondents report that two-thirds of these audits were performed by independent, third-party auditors or consulting services, which is a positive sign that companies are adopting an important separation of duties to ensure audits aren't being conducted by the same IT staff members who manage systems.

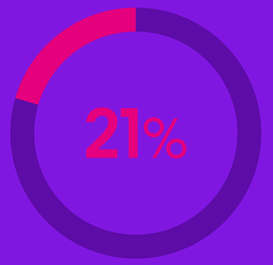
Even if not compelled to do so by regulations, it is only prudent that every organization performs an internal security audit or a risk assessment at least annually. It is encouraging to see in our survey that 75% of respondents said their company conducted internal security audits on their IBM i systems at least once per year, with about two-thirds of those doing audits every six months or more frequently. 19% say their company had failed an internal security audit, which hopefully initiated actions to better secure IT systems.

Areas cited most often by our survey respondents as being examined during their audits of IBM i security are system access controls, data access controls, application security, passwords, and network security. A couple of the areas least examined in audits that are cause for concern are mobile devices and security breach-response plans. The former reveals a vulnerability at endpoints — an all too common weakness exploited by hackers, and the latter exposes organizations to additional expense and disruption due to an inefficient response should a breach occur.

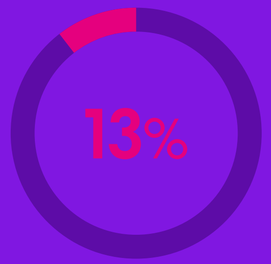
Frequency of compliance audits



Annually

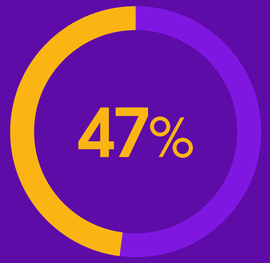


Semi-annually

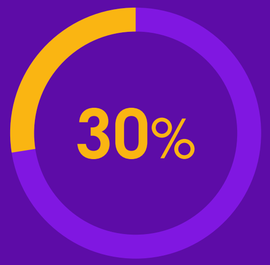


Quarterly

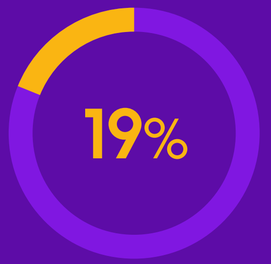
Primary responsibility for compliance audits



Third Parties



Internal Staff



Consultants

Primary responsibility for compliance audits

Annually

Semi-annually

Quarterly

Monthly

16%

Failed a Compliance Audit

19%

Failed an Internal Security Audit

Top areas examined in audits:

58% - System Access Controls
52% - Data Access Controls
52% - Application Security
47% - Passwords
47% - Passwords
46% - Network Security

Security Breach Impact and Response

Of the companies we sur veyed this year, 42% said they have experienced at least one breach of their computing systems during their history. Of those who reported a breach in the past year, the majority had experienced more than one breach during that twelve-month period. Considering this, one wonders if organizations that have experienced one breach are predisposed to more.

In another question from our sur vey, 24% of companies that have experienced a breach reported that at least one breach was undetected for two months or longer. This underscores the importance of having systems, processes, and policies in place that can quickly detect a breach, as well as the necessity of performing regular, in-depth security audits. Of course, the longer a breach goes undetected, the more damage that can potentially occur, especially if sensitive data is not encrypted. In fact, our survey showed that the 20% of those experiencing a breach had unencrypted data stolen, with nearly half of these incidents involving personally identifiable information.

42%

of respondents say their company has experienced at least one breach

24%

of breaches went undetected for two months or longer

20%

of breaches resulted in theft of unencrypted data

31%

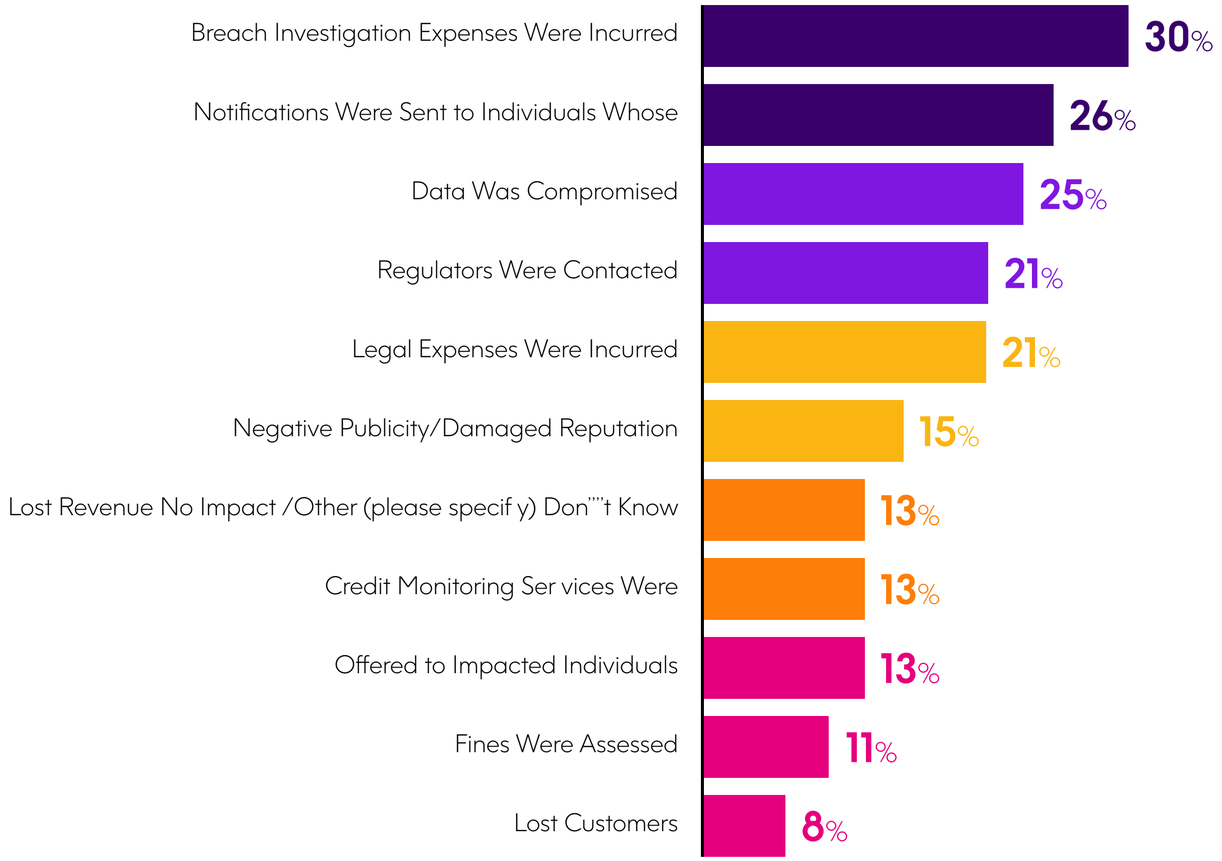
of breaches were attributed to an internal staff member or contractor

In addition to sending out breach notifications and notifying regulators, our survey respondents reported many other painful business impacts from breaches that are shown in the chart on this page.

Finally, it's not unusual for breaches to be caused by actions within the organization, whether through malice or negligence, with 31% of breaches reported in our sur vey being attributed to the actions of an internal staff member or contractor. **A 2019 data breach study conducted by Verizon** based on over 2,000 recent data breaches showed that 34% of cyberattacks in some fashion involved the activities of internal actors. This makes clear the necessity of implementing strong system and data access controls, and for users to receive ongoing training so they don't inadvertently disclose sensitive information, fall prey to phishing tactics, etc.

What regulations must your organization adhere to?

Choose all that apply.



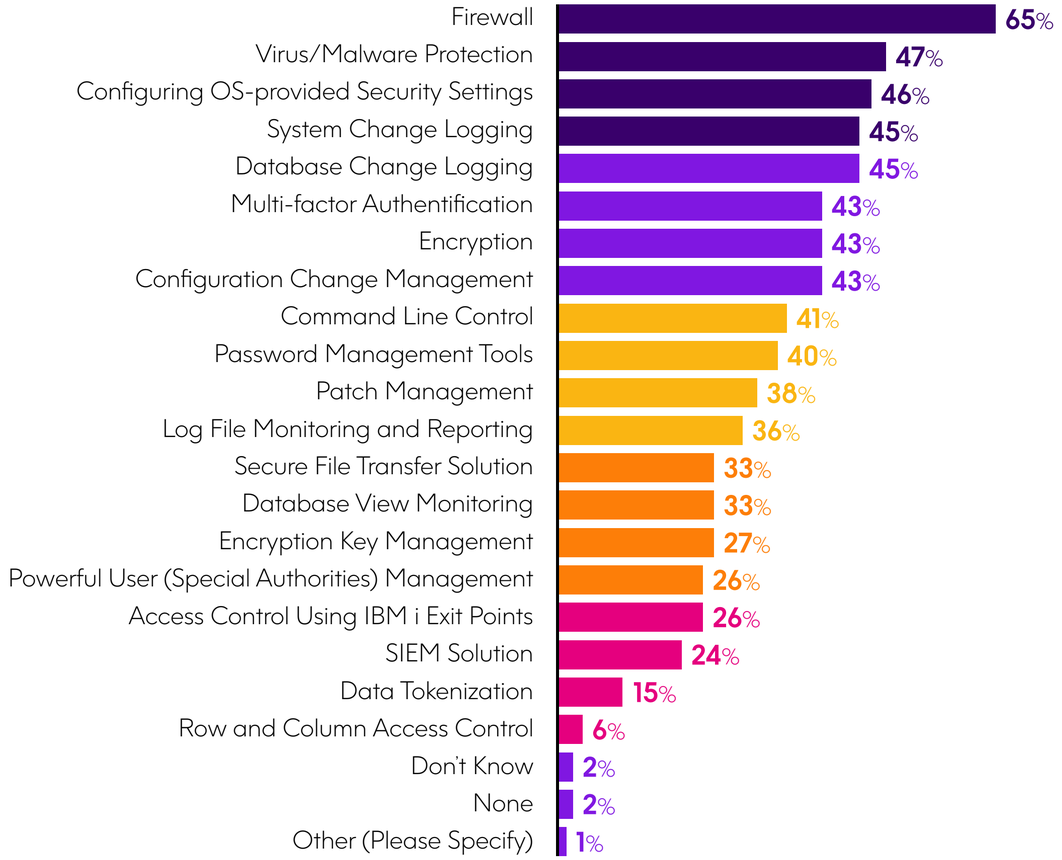
Note: Respondents were asked to "select all that apply;" therefore, figures don't total to 100%.

Present and Future Investments in Security and Compliance

In this final section of our report, we take a look at what respondents had to say about their company 's current investments in security and compliance efforts as well as the IBM i security measures their company plans to invest in during the coming year.

Regarding current investments to meet compliance regulations and prevent a breach, those related to firewall and anti-virus were at the top, but close behind were investments related to management of OS-provided security settings, system change logging, database change logging, multi-factor authentication, encr yption, and configuration change management. When compared to the results of this same question last year, there were a couple of notable year-over-year changes: database change logging grew from 27% to 45%, and multi-factor authentication grew from 35% to 43%.

What security measures has your organization invested in today to meet compliance requirements and prevent data breaches? Choose all that apply.

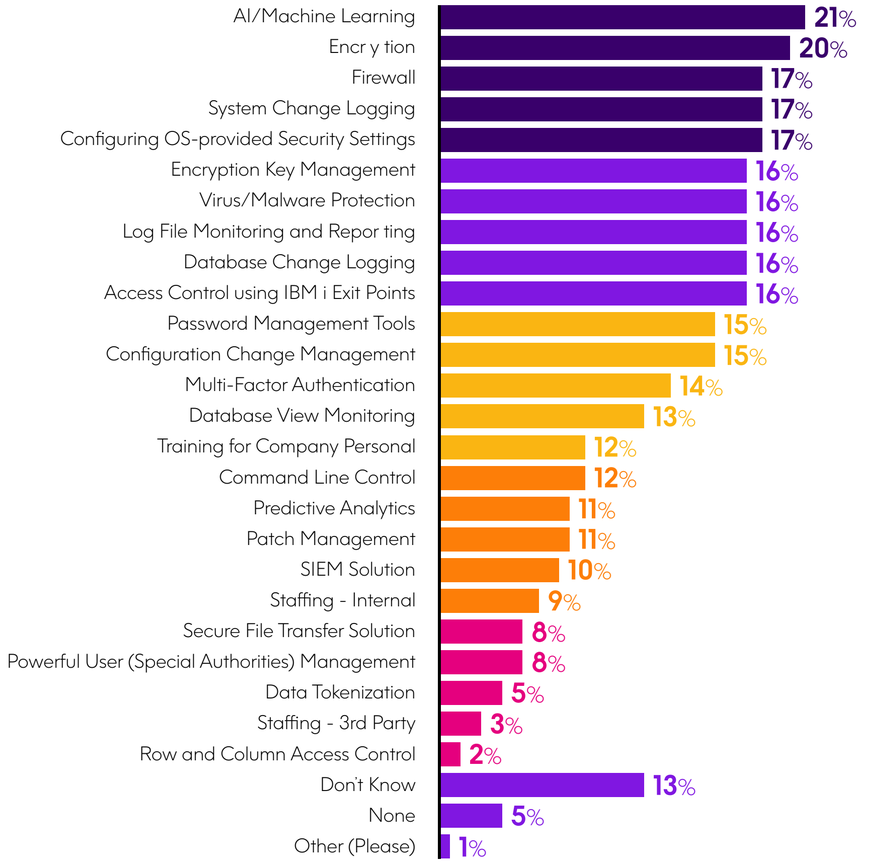


Note: Respondents were asked to "select all that apply," therefore, figures don't total to 100%.

Regarding future investments in IBM i security measures, AI/machine learning was the most cited at 21%, which increased significantly from the 9% reported last year. It's clear that IT managers are starting to pay attention to how these advanced capabilities can reduce security incidents and are looking to include them in their future technology investments. Security Information and Event Management (SIEM) solutions, particularly those that include next-generation analytics, are at the forefront of this capability as they not only aggregate and analyze security events to provide alerts, but can also predict vulnerabilities. In our question about current security investments, 24% reported their company has a SIEM solution installed. When those respondents were asked which SIEM is in use, Splunk was the most cited at 30% followed by SolarWinds, QRadar, Fortinet, and MacAfee with 24% or greater.

Encryption was close behind AI/machine learning as a top choice for future investments with 20% of respondents indicating this data-obscuring technology would be procured during the coming year. In light of what has been described in the previous pages of this eBook about the per vasiveness of sensitive data on IBM i, the impact of breaches, and the growth of compliance regulations, it makes sense that an increasing number of companies are looking to invest in this critical technology.

In what IBM i security measures will your organization invest in the coming year? Choose all that apply.



Note: Respondents were asked to "select all that apply," therefore, figures don't total to 100%.

Conclusions

Our survey this year leaves little doubt that IT security and the burden of meeting compliance regulations weigh heavily on the minds of those who manage IBM i systems in their organizations. Their level of confidence to protect systems and achieve compliance is slipping as threats continue to grow, regulations continue to proliferate, and other IT challenges continue to mount. Fortunately, we are also seeing a notable increase in the awareness of security issues and approaches, along with a corresponding willingness to be proactive in fighting security threats through regular internal-security audits, the procurement of new technologies, the addition of IT security staff and third-party experts, and the expansion of security-related training for existing IT staff and end-users. With this added vigilance, IBM i shops have their best shot at preventing IT security issues from impeding the smooth operation of their organizations

Precisely Can Help

With proven security solutions for IBM i and a deep bench of experts whose focus is to stay up to date on security vulnerabilities, best practices, and mitigation technologies, Precisely is here to help you enhance your IBM i security.

Precisely Security Software for IBM i

Strengthen your system-access security, file and field security, and security monitoring and auditing with our best-in-class software solutions that cover:

- Control of network access, database access, and command access
- Encryption, tokenization, and anonymization
- Secure file transfer
- Elevated authority management
- Multi-factor authentication
- System and database monitoring and reporting
- Model-based compliance management
- SIEM integration
- And more

Precisely also offers solutions and ser vices for AIX, Windows, and Linux that address security and compliance-auditing needs.

Precisely Professional Services for IBM i

Our security experts are here to assist your team in reinforcing your layers of IBM i security in numerous ways by:

- Performing in-depth, periodic risk assessments on your IBM i environments. Using detailed findings from the assessments, we'll sit down with your IT and compliance managers to help formulate and implement a plan for remediating discovered vulnerabilities.
- Providing managed-security services that give your company dedicated IBM i security experts who, depending on the level of service chosen, regularly check security configurations, deliver status reports, monitor systems 24x7 for security events, adjust security configurations, and more.
- Assisting your team during compliance or security audits by generating reports required by your auditors.
- Ensuring a successful implementation of Precisely security technologies and providing all needed training.

To learn more about all of our security products and services, visit **www.precisely.com**.

precisely

About Precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely's data integration, data quality, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

www.precisely.com