Infosys cobalt

VIEW POINT

SECURE OFFBOARDING - AN INTEGRAL PROCESS TO ALLEVIATE RISKS

Abstract

In today's technology driven ecosystem, organizations focus more on onboarding the employees with their well-defined process to ensure secure access provisioning and formalities. However, organizations tend to undervalue the offboarding process driven by their siloed departments and lack proper control mechanism. Ideally, a well-managed offboarding process should ensure smooth, secure, and risk-free transition from former employee to next. This POV discusses the various security risks associated with the offboarding process, mitigation techniques, and best practices for continuous improvement. It also shares some of the best practices to fortify organizations against security flaws associated with employee terminations and movements.

Infosys®
Navigate your next

Introduction

In the swiftly digitizing landscape, corporate environments are increasingly adopting hybrid work models, Bring Your Own Device (BYOD) policies, and cloud-based storage solutions. Alongside, there is a surge in Software-as-a-Service (SaaS) applications accessing sensitive data. This paradigm shift introduces heightened vulnerabilities, threats and the need to combat malicious actors.

As per WEF's Global Cybersecurity Outlook 2024, emerging technologies like Generative AI will worsen long-term challenges related to cyber resilience.

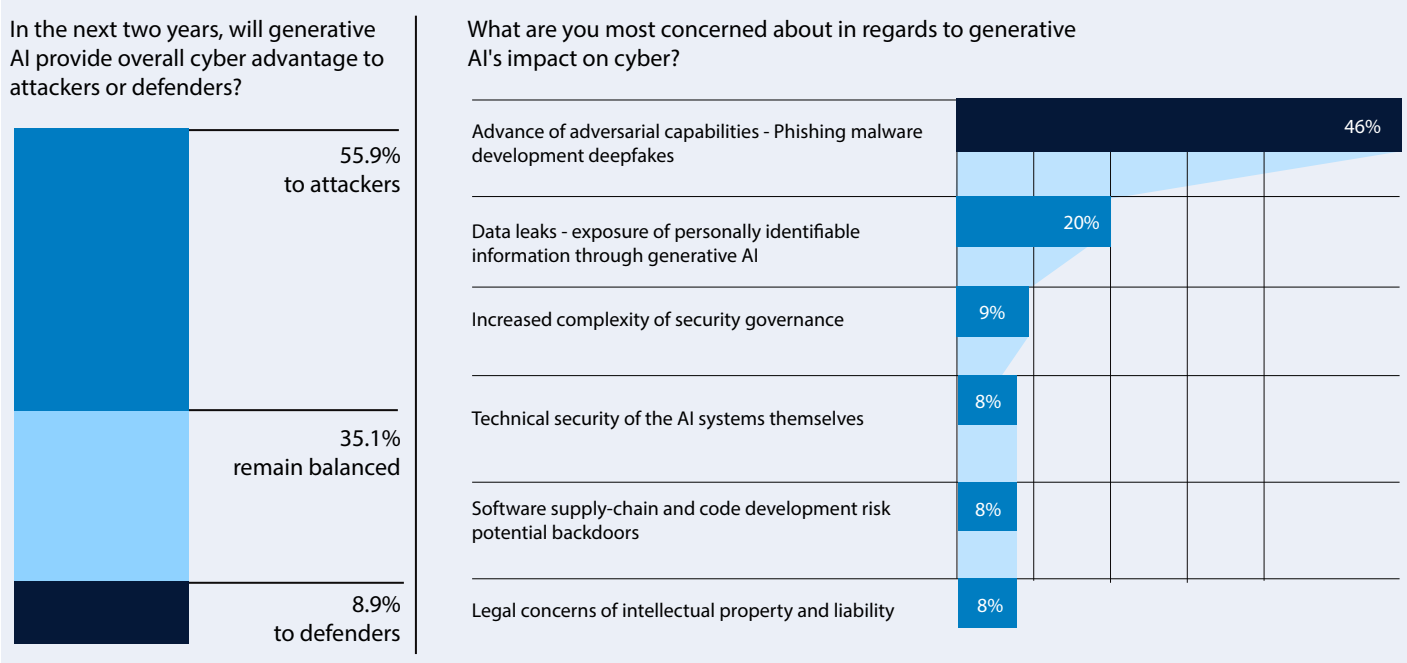

Figure 1: Generative AI impact on cyber resilience [1]

Organizations must assess the short-term, mid-term and long-term implications of modern technologies like Generative AI on their cyber-resilience posture. According to a recent survey of cyber executives, approximately 50% of the executives think that Generative AI will have strong impact on adversarial capabilities (such as phishing, malware, deepfakes). Additionally, below statistics illustrates the adoption of cyber insurance based on revenue and number of employees.

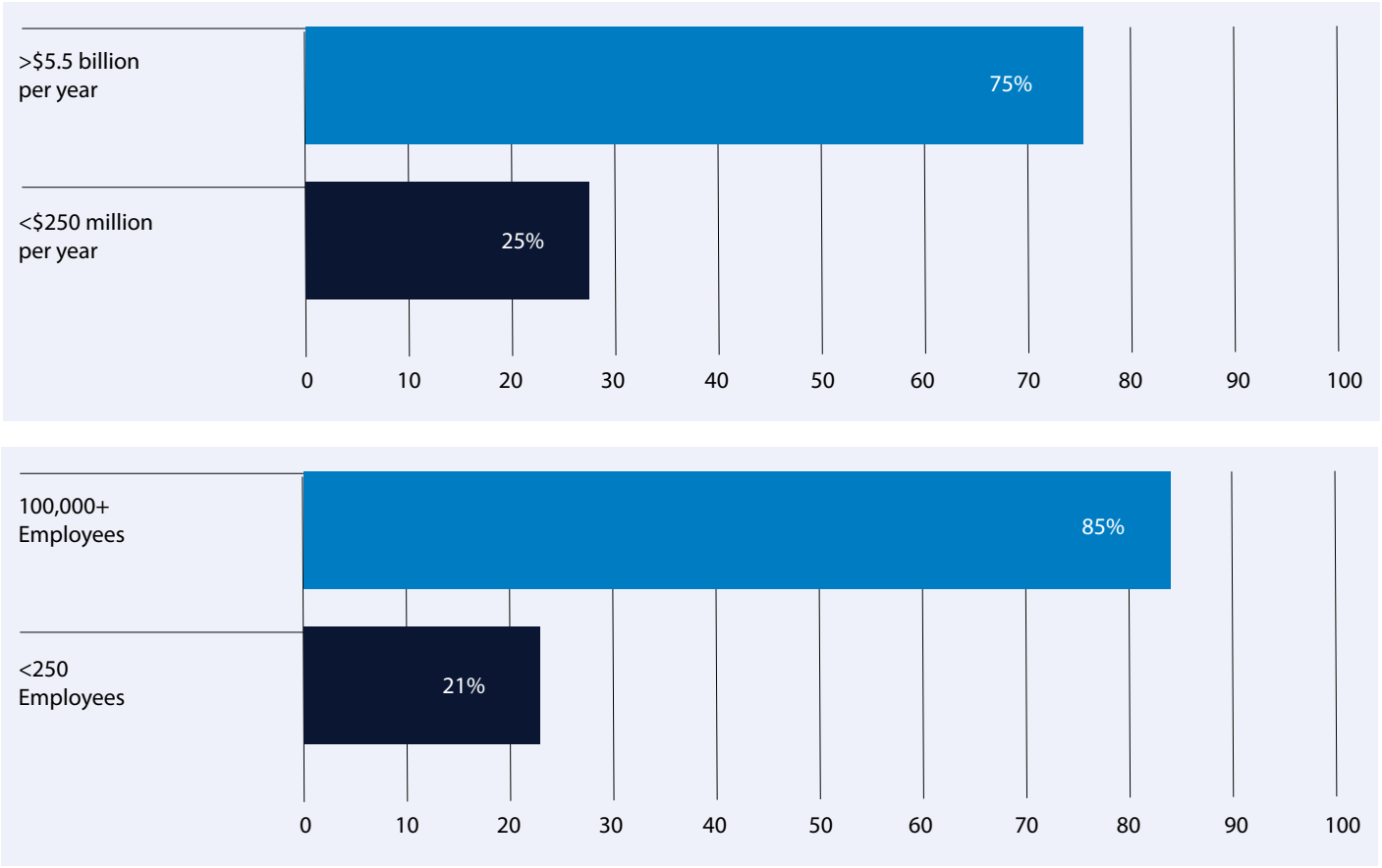

Figure 2: Cyber insurance by revenue and number of employees [1]

As per 2024 organizational cyber resilience trend, the below statistics clearly depict that 22% of respondents are optimistic that the cyber governance and culture will improve in the next couple of years.

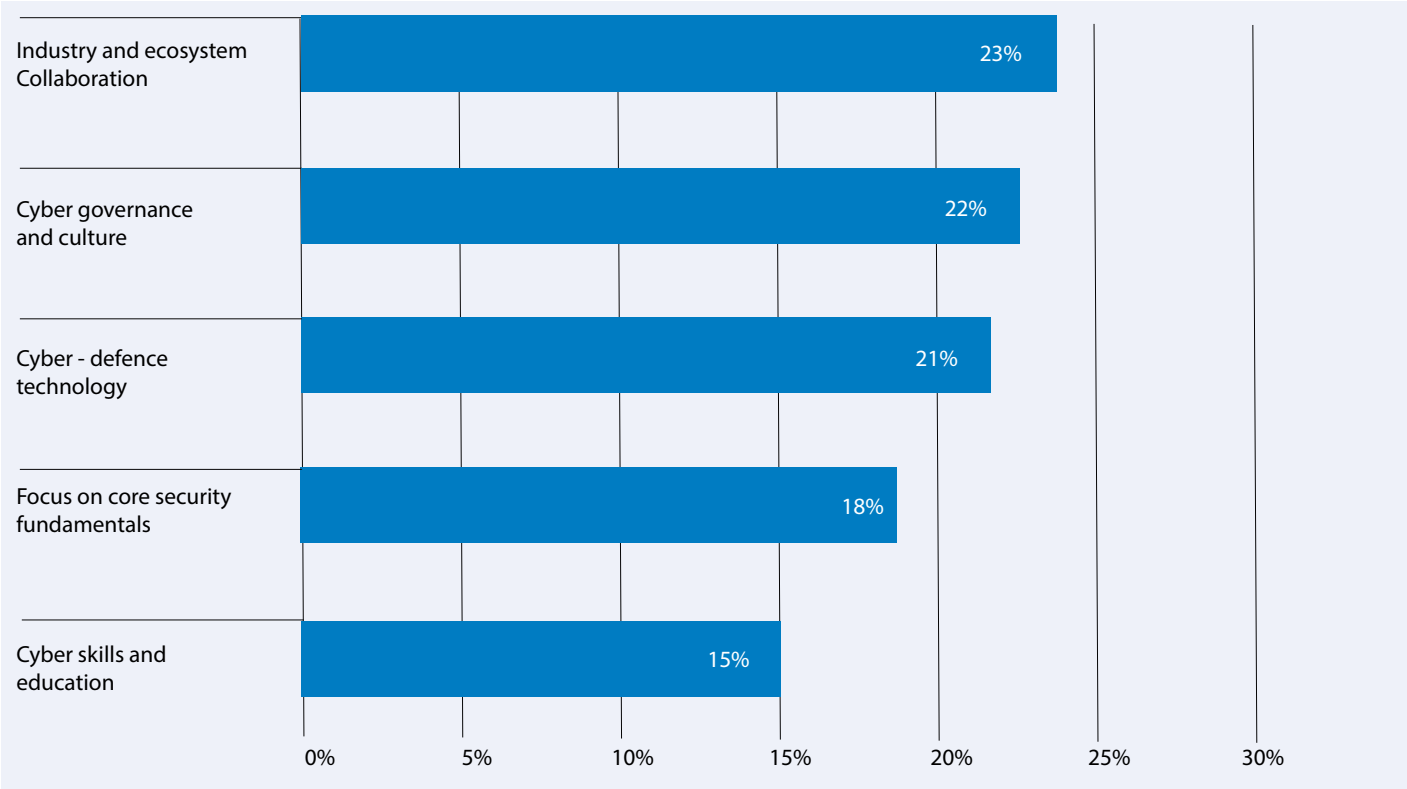

Figure 3: Cyber resilience key factors [1]

In the hybrid workforce models adopted by organizations, the security of data and related systems hinges on the effectiveness of employee onboarding and offboarding processes. The onboarding process provides the first opportunity to inculcate organizational culture and security within new joiners. A robust onboarding process can promote adherence to organizational policies and data security norms throughout their tenure. Conversely, offboarding is critical to ensure smooth transitions for departing employees. A systematic offboarding procedure helps mitigate risks as data leakage, unauthorized access, compliance violations, etc. it ensures timely revocation of access for ongoing security measures.

Employee onboarding and offboarding is crucial for data security due to the following reasons:

- **Managing access and authorization to sensitive information**
- **Ensuring compliance with regulatory standards**
- **Reinforcing organizational security policies and culture to counter threats**
- **Minimizing vulnerabilities**

Onboarding process – More focused and well-organized

After recruitment, the employee lifecycle involves induction and onboarding, where access to necessary systems, applications, and databases is provided for work activities. Moreover, vendor partners or SOW contractors require access to conduct their tasks according to SLA agreements. Organizations must establish a well-coordinated onboarding process involving HR, Finance, IT, and other departments to help new employees adapt quickly to their roles. Each department aims to ensure new joiners feel welcomed and comfortable while emphasizing security best practices for a seamless integration into the organization's structure.

Offboarding process – Siloed and less coordinated

Many organizations overlook the importance of the offboarding process compared to onboarding. Offboarding procedures are often fragmented across departments, lacking coordination and leaving security risks unresolved. Employees and vendors retain access to sensitive information, requiring timely access revocation upon separation to avoid audit findings. It's crucial for organizations to conduct secure offboarding in compliance with security and corporate policies.

Factors contributing towards ineffective offboarding

As per a recent industry security survey, security teams neglect collaborating with HR and Risk and Compliance Management teams leading to ineffective and disorganized offboarding processes. Most organizations prioritize training and benefits over other factors to enhance employee experience.

The top contributing factors to an unorganized and ineffective offboarding process are:

- **Lack of coordination between departments:** Typically, the HR team leads the offboarding process. However, all associated teams should collaborate to ensure complete access revocations for a smooth departure. Record keeping is essential for auditing and compliance across the organization, especially with remote and hybrid work setups.
- **Inadequate training for managers:** managers lack comprehensive training on handling the offboarding process. It is important to educate the managers on how the process fits in the organization. With remote working and hybrid working model, workers need to return the hardware asset to the organization and perform due diligence checks.
- **Leadership prioritizes more on skills enablement and employee experience:** the leadership team is more focused on training and fostering employee experience. This is a key factor to ensure attrition rate is under control.
- **Insider risks due to poorly managed offboarding process:** The risk from people inside the organization during their during departure from the company contributes to insider risk. As per a recent industry survey, 44% of the people at the helm of various security practices experienced incidents pertaining to malicious intent from insiders who are departing the organization. Treating employees when they separate from the organization can be a crucial factor to reduce such insider risks. Proper training given to the offboarding team can ensure that they give due respect and empathy to employees during their departure. These measures can drastically reduce resentment from separated employees.

Setup a secure offboarding process

An offboarding process should include the security and risk elements upfront. This requires building a team of well-trained HRs and associated departments, an organized workflow integrated with technology solutions, and giving due respect and empathy to the departing employee.

- **Brainstorm, develop detailed workflow, and provide training to departments:** The leadership team from HR, security, and associated departments should brainstorm and provide use cases to frame a workflow for employee termination and movements. The workflow should incorporate necessary logic on the reason for separation whether voluntary, involuntary or any reason. The workflow should clearly have insights on the details pertaining to access revocations to account level, application/system/database levels, recovering business data from employee physical assets, employee settlements, exit interview forms, employee termination and non-compete agreements. People managers and associated departments involved in offboarding should thoroughly understand process workflow in a contextual manner.
- **Integrate technology solutions to reinforce consistency in onboarding and offboarding process:** Organizations should give equal significance to offboarding as onboarding process. Ideally, the offboarding process should leverage technologies to ensure the access across applications/systems/databases, smart card access to buildings/server rooms are revoked on time and tracked/recorded in the employee offboarding process workflow systems. Technology solutions including IAM tools must be integrated to the unit level HR systems to ensure access revocations are based on the separation date. The process starting from resignation notification email should feed into HR application and the necessary departments to initiate the offboarding access revocations. The siloed systems/processes can correlate with technology platform solutions to create end to end processes.
- **Cloud/SaaS usage permissions up to date detailed list maintenance:** With organizations adopting SaaS applications, it is imperative to keep track of the SaaS usage of departing employee and maintain an active documentation include the list of all Cloud/SaaS platforms utilized by the organization including the access levels each employee have is essential. Cloud Permissions Management (CPM) or Cloud Infrastructure Entitlements Management (CIEM) can help the security team to discover all permissions to cloud assets for a given identity within an organization and remove them as required.
- **Monitor anomalies in activity of outgoing employee:** User Entity Behavioral Analytics (UEBA) can help the security team to monitor and flag anomalies in activity to stay ahead to potential threats or data loss scenarios. The security teams can continue to monitor activity at the last few weeks of notice period of the employee's departure date. A retrospective check of activity of the departing employee can help to identify any potential risks.
- **Protect Intellectual and Physical Property:** With remote and hybrid work models in place, the physical assets are out of control. It is important to protect the intellectual property of the devices. Implementing Data Security Platform (DSP) solutions from vendors can enable monitoring, protect business information, and help in recovering data before employee separation. Device management solutions can lock devices and help in erasing the data completely, even on devices that are offline and not reported to management server at the stipulated time. Most organizations as part of asset recovery, after the employee termination, reset devices to default configuration and delete corporate data. To prevent potential data loss, it is necessary to enforce device lockdowns on sharing files with personal webmail and USB ports. To prevent access to applications and devices, it is necessary to turn off the Single Sign-On (SSO) feature. For privileged accounts, the password can be reset and remove the main directory account access.

Security controls effectiveness for terminations and movements

A recent survey from Forrester Research provides insights on the interconnection between data breaches and immaturity of organization's Identity Governance solutions. Most of the organizations devise an integrated platform approach for Identity Access Management (IAM) and Privileged Access Management (PAM) to achieve uniform access control policies thereby improve operational efficiency.

Most organizations, specifically public limited companies, heavily invest on regulatory compliance, to ensure brand reputation and increase investor confidence. Major compliance frameworks, standards, and regulations mandate the need for user access reviews and other necessary security controls to ensure access revocations during terminations or movements within business units timely and accurately. The business units within organizations should adhere to User Access Review controls for compliance with regulatory requirements.

IAM tools from vendors for conducting User Access Reviews can simplify the entire employee access audit trail. The audit team gets reports as evidence on the access revocations for terminated and movements in different units. Manager access approvals and termination and movement dates from HR reports should ensure no anomalies in access revocations for all terminated and unit movement users. From a compliance perspective, most business units have internal auditing and external auditing carried in predefined timeline to ensure the design and operating effectiveness of the security controls.

Way forward

A well-structured and graceful employee offboarding experience can unlock multiple advantages to the organization

- Proper handoff, cancellation and revocation of access can help in improving security of sensitive information and data
- Perform internal auditing for all terminations and movements in the organization to ensure compliance with internal security controls in place for policies and procedures
- Successful offboarding with exit interviews will educate people managers, HR, and related departments on key aspects like what is going well, what did not go well, scope for improvement for next recruitment
- Proper closure of employee contracts helps mitigate legal threats
- Provide former employees a respectable signoff so that they can serve as a good brand ambassador for your company's reputation
- Ensure asset tracking and return by leaving employees ensure that data is not accidently shared or distributed

The offboarding checklist provided below gives a tactful, effective offboarding best practices.

- Thank leaving employee for the contributions and give due respect to their contributions.
- Ensure knowledge transfer with proper documentation and hand over to the replacement resource.
- Capture reason for separation and edit or update the offboarding process workflow.
- Formal communication to the rest of the company regarding employee departure.
- Secure back the company assets, Revocation of access from systems/applications/databases.
- Exit Interview to gather insights and use it as a tool for continuous improvement process.
- Stay in touch with the employee with a well-managed alumni group for suggestions and improvements.

Conclusion

In today's digital business ecosystem, organizations are more focused on employee experience and skill enrichment as the major drivers for brand building and financial growth. Most organizations have a well-structured onboarding process with access provisioning to induct new employees into business units. However, undervaluing the offboarding process can unfold security risks that can affect the brand reputation. Employee experience must be consistent throughout the lifecycle (from onboarding and offboarding). Integrating technology solutions in employee offboarding can ensure addressing the security risks associated with various system access. Auditing the employee terminations and movements from HR reports and application system level can help organizations to attain a more mature security posture.

The leaders need to provide equal focus to onboarding and offboarding process and should regularly review the offboarding process to understand pain points, potential risks, and vulnerabilities. Offboarding strategy is a contributing factor to cyber resilience and can affect the brand reputation. The budget invested on cyber insurance percolates down to the offboarding process to ensure that your organization is cyber resilient in all departments.

References

1. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
2. https://www.sailpoint.com/identity-library/securing-your-enterprise-with-identity-governance-and-pam/
3. https://www.forbes.com/advisor/business/offboarding/
4.https://www.okta.com/resources/whitepaper-top-5-reasons-to-automate-identity-lifecycle/
5. https://www.codemonk.ai/insights/securely-onboarding-and-offboarding-employees
6. https://www.forrester.com/report/best-practices-for-securely-offboarding-employees/RES179056?ref_search=0_1706827775318
7. https://www.beyondidentity.com/blog/cybersecurity-risks-improper-offboarding-after-layoffs
8. https://www.csoonline.com/article/575071/top-risks-and-best-practices-for-securely-offboarding-employees.html

Author

Roshan Hareendra Babu

Senior Consultant

Roshan is a Senior Consultant in Cybersecurity with more than 13 years industry experience. He has strong expertise in GRC practice and has led multiple projects in North America and Europe regions. His core focus areas are SOX ITGC, ISO 27001, NIST-CSF, Risk management.

For more information, contact askus@infosys.com

Infosys®
Navigate your next