protiviti®

Face the Future with Confidence

Data, Application & Infrastructure Security Risk Assessment

Internal Audit, Risk, Business & Technology Consulting

Let's Explore the Iceberg!

Understanding gaps in how your applications and infrastructure protect your data is a priority for both Operations and Executives.

Application Interface is only the tip of the Iceberg

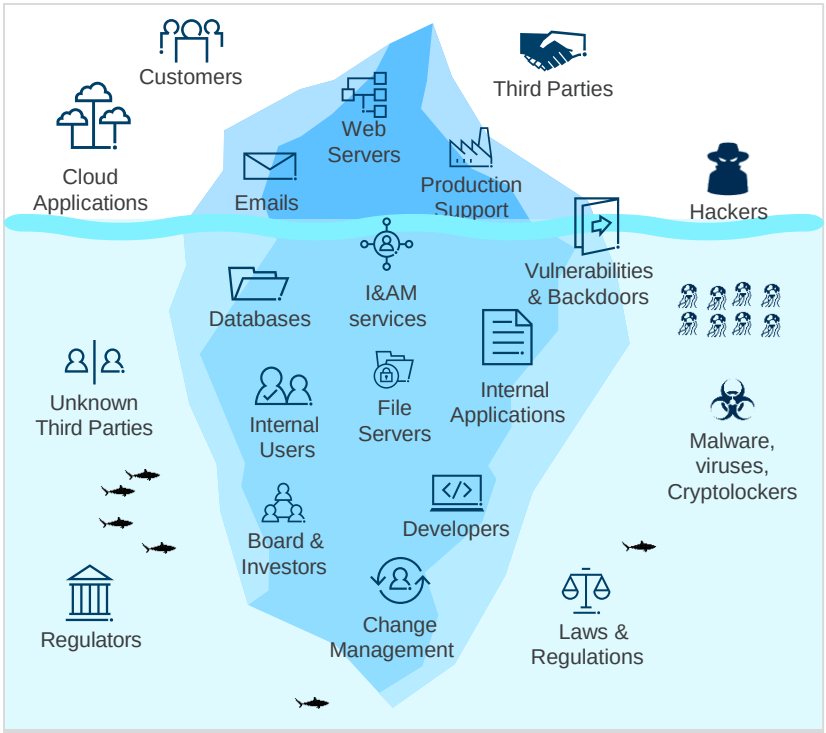
Application are interfaces used to access and process data (business or personal) and are only the visible part of a more complex IT landscape.

An effective cyber security programme needs to address the issue of data, application and infrastructure security. Traditional approaches have relied heavily on technical penetration testing of application interfaces and their underlying hardware and networks. While penetration testing can be effective at identifying risks from the threat perspective of a cyber-attacker, it cannot provide coverage of many other key security-focus areas within the business ecosystem.

In fact a 360° approach is required to assess aspects such as user authentication, access management, data flows, development lifecycle, logging and auditing, application platform resilience, data protection, etc. Such an approach includes identifying the weaknesses of any stakeholders' risky behaviours.

The approach should be based on a recognised security framework and regulations (NIST, ISO, ENISA, ANSII, GDPR) and completed with technical security assessments of network, connectivity, hosting, databases, computers and mobiles devices together with the overall process involving their management.

⚠ Classical penetration testing scope allows only to view the tip of an iceberg!



The submerged part of the "IT Iceberg" hides many risks and cybersecurity issues

Key Challenges

- Enormous appetite for new and acquired applications outpacing organisations' ability to keep up with the risks
- Attitude to internal application security must change to assume that attackers are already inside
- Lack of current and accurate application inventories
- Increased desire to share data with business partners adds risk
- Shortage of skills and capabilities to keep up to date and defend
- Embedding security in the software development life cycle (secure SDLC)
- The ever-changing environment requires sustainable awareness of cybersecurity risks at all levels of the company

The majority of the application data, interfaces, systems, processes, laws, regulations, third parties, and users are usually out-of-scope.

Where to Start

Deciding on a course of action is only the start of the challenge:

- Organisations can often have hundreds or thousands of applications in active use.
- This creates complexity, and from complexity arises uncertainty
- Large numbers of applications, with sizeable numbers of users, and multiple interfaces, both internally and externally, create a perfect breeding ground for major security risks.
- Already, organisations are struggling to appropriately staff information security functions. As the pressure and load of focusing on day-to-day tasks mounts, little time is available for strategic risk assessments of hundreds of applications.
- A structured, thorough and managed assessment approach is vital to ensure that the security risks of these applications to the business are identified in a cost-effective, demonstrable and sustainable manner.

Getting Below the Surface

How well do you know your IT architecture?

The following questions are useful in considering your application's and infrastructure security assessment programme maturity:

- Do you have a current, accurate and single source of all application assets with an owner?
- How do users gain access to applications? How do you determine their business need to do so?
- What sensitive data is leaving your organisation? Is it transferred securely, and can you track who transferred it?
- Are your cybersecurity policies compliant with regards to local, European and international norms, standards and regulations?
- How well do you know the security of your Third Parties and externals interacting with your systems?
- How robust is your network, on premise and cloud hosting? How you tested your cyber resilience plan?
- Are your processes and systems Secured by Design?
- Have you identified your risky processes with regards to current regulations?
- Do your employees benefit from regular IT and Cybersecurity risk awareness training ?

Three Solutions to Meet your Needs

1 Data and Application Security Risk Assessment

Organisations require a broad and deep assessment of their application estate that is focused on identifying material and realistic security risks that pose a tangible impact to their business in terms of reputational damage, direct financial loss, legal action and regulatory sanctions and scrutiny.

Building an effective Data and Application security risk assessment programme is critical in order to accurately assess their risk exposure and to demonstrate to boards and regulators that they are pro-actively managing same.

Protiviti has developed a highly effective Data and Application Security Assessment programme which has been proven to identify significant risks throughout the full scope of an application's lifecycle.
Our methodology can be applied in situations from single application instances right up to hundreds or thousands of applications.

2 Infrastructure Risk Assessment

Similarly to Data and Application Security Risk assessment, Protiviti has developed an Infrastructure Security Risk Assessment programme which has been proven to identify significant infrastructure risks.

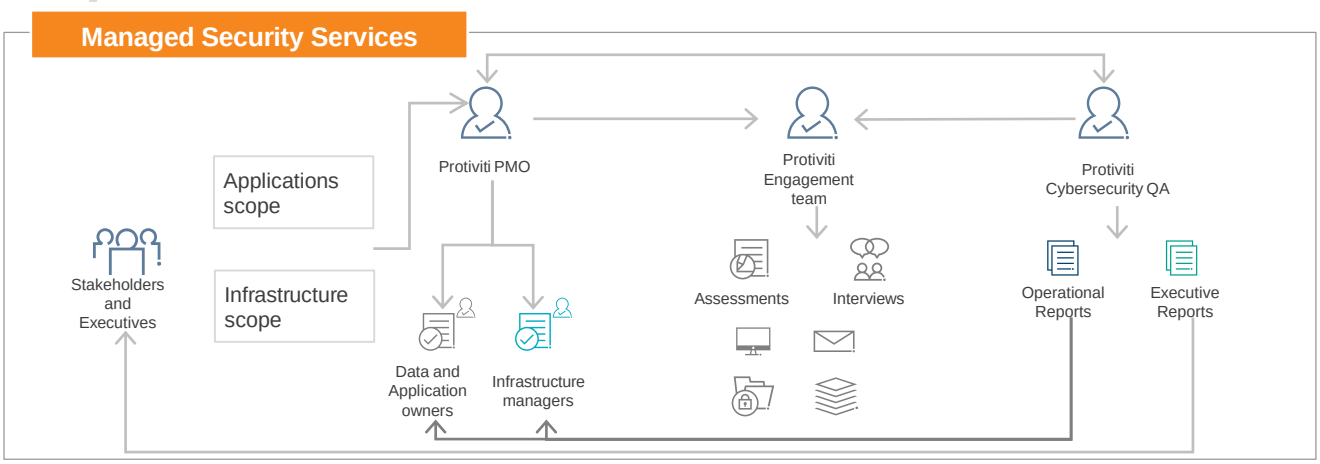
Our methodology can be applied for internal clients on premise infrastructure hosted locally and internationally as well as cloud hosted.

Infrastructure Security Risk assessment also covers security assessment of fix terminals and mobile devices as well as connected objects to the enterprise network.

3 Protiviti Managed Security Services

For larger programmes, our Managed Security Services is a proven solution for mobilising, managing and executing large-scale, multi-year, global coordinate data, application and infrastructure security risk assessments.

Our clients gain the benefit of having access to Protiviti Global Network of highly qualified cybersecurity consultants and legal team, coupled with an experienced and dedicated cybersecurity PMO and a centralised cybersecurity QA function to ensure consistent quality.



Data, Application and Infrastructure Security Risk Assessment

Face the Future with Confidence

Contacts

Nuvin Goonmeter

Managing Director
nuvin.goonmeter@protiviti.fr

Anis Hammami

Manager
anis.hammami@protiviti.fr

protiviti.fr

PRO-013119

protiviti®