



Cyber Response Services



Executive Summary

The Problem

Higher Education is facing an existential threat from malicious cyber actors and has focused attention on cybersecurity to prevent and recover from incidents ranging from negligent error, such as accidental data breach, through to malicious intent and data theft.

“It can pose existential threats to any organization — large or small, public or private...if you cannot operate your business, if you can’t operate your college, then you may not be able to exist.”

- Henry Stoeber,

President and CEO of the Association of Governing Boards of Universities and Colleges



The Solution

- Prepare for an incident by ensuring your organisation is fully prepared in the event of a cyber-attack.
- Providing an expert incident response service to help safeguard your IT and OT assets during and after an attack.
- Supporting the fast recovery and restoration of your systems and services, and helping to identify key improvement areas to your cyber capability through lessons learned.

Why KPMG?

KPMG can support in all aspects of the incident lifecycle using certified experts with extensive backgrounds in incident response. KPMG is a 24/7/365 global IR service provider with the capability to quickly get resources on-site whenever and wherever we are needed. With our vast reach of alliances and experience, our teams are adaptable to work with our client’s existing environment, technology and tooling to ensure a safe and professional transition from crisis to recovery.

Cyber security – A board level risk

Everyone is affected by cyberattacks in our fast changing, hyperconnected digital world. With more funds at hand, attackers are employing modern techniques such as machine learning and cloud computing to find novel ways to attack organisations. Keeping attackers at bay is becoming increasingly difficult.

In the KPMG Global CEO outlook survey 2022, cyber breaches were identified as the top concern of CEOs. As part of their digital transformation programs, CEOs are looking for stronger partnerships to maintain cyber resilience. With our incident response retainer program, we help organisations establish the partnerships they need to succeed in their transformation efforts.



Business resilience

It is evident that attackers will maintain an edge over your defences with the recent increase in zero-day vulnerabilities, so it is essential that you have a resilient approach to coping with cyber attacks, especially events that disrupt business services and force a company wide response.



Ransomware attacks

Computer malware can disrupt or shut down a company's operations when it encrypts critical business systems. Ransom demands can range from hundreds of thousands to millions of pounds.



Global economic and political situation

While the global pandemic pushed your capabilities for how you could use technology, cybercriminals and state sponsored attackers have also increased their activities, raising the associated risks in cyberspace. Due to the value you place on technology, cybercriminals and state-sponsored attackers are increasingly targeting systems.



Internal Threat

The breach of trust by employees and contractors can compromise competitive advantage. Every year, courts evaluate evidence of employee misconduct and theft of intellectual property. Companies require support from forensic investigators to address these cases.



'2022 Global CEO Outlook'

[KPMG 2022 CEO Outlook - KPMG Global \(home.kpmg\)](#)

You're in safe hands

With cyber security threats increasing in size, complexity and maturity, effective incident response is a critical business asset to an organisation. The client's experience during any one incident, regardless of how big or small, is not a comfortable situation. As part of KPMG's engagement process, our teams actively solicit feedback during every engagement. Client feedback is reviewed at all levels, including the lead client account team, in an effort to manage client expectations, satisfaction and build long standing relationships.



Global Coverage

Our cybersecurity consulting practice is among the largest in the world, with cyber response members located around the globe. Our 24/7 support service means that you'll have industry experts on hand no matter when or where an incident occurs.



Sector Insights

Our clients come from diverse industries and sectors, and we have gained a deep understanding of what's critical for them within their sectors - especially which data assets and processes create value for them, and which may hold value for threat actors.



Technical Prowess

It's critical to have expertise when it counts. The breadth of our team's expertise in all aspects of cyber security allows us to provide the highest quality of service. When needed, we can provide our own security tools or make the most of yours. Custom-developed tools, scripts, and licensed security products are part of our toolkit.



Our Alliances

Together with our digital partners, we provide services that give us a competitive advantage. KPMG leverages technology from a number of industry leaders.



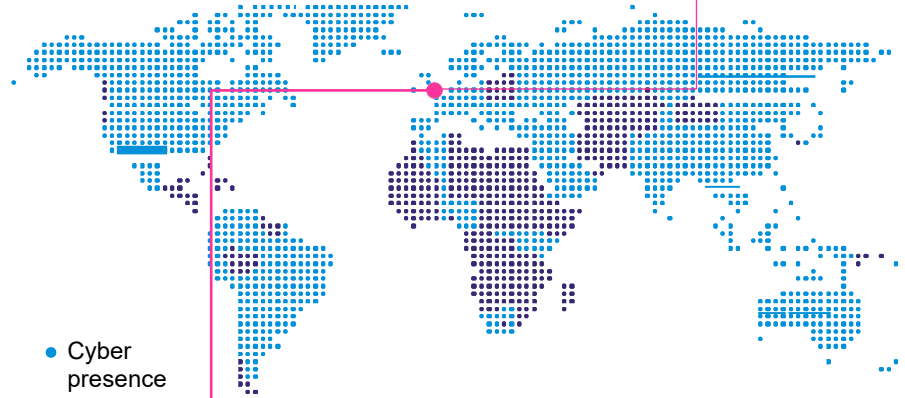
Regulatory coverage

Our firm's comprehensive understanding of regulatory requirements in multiple jurisdictions allows us to assist our clients in clarifying their concerns regarding subject notification, liability, and business resilience.



Our cyber security delivery capability

Our global footprint



KPMG has offices in all major cities and locations within United Kingdom. This gives us the capability to deploy resources concurrently if required, including co-locating resources where required.

- | | | |
|-------------------|-------------------|-------------------|
| Birmingham | Glasgow | Nottingham |
| Bristol | Leeds | Reading |
| Cambridge | Liverpool | |
| Cardiff | London | |
| Edinburgh | Manchester | |

North America

850+

EMEA

1500+

A global network consisting of
3200+
professionals

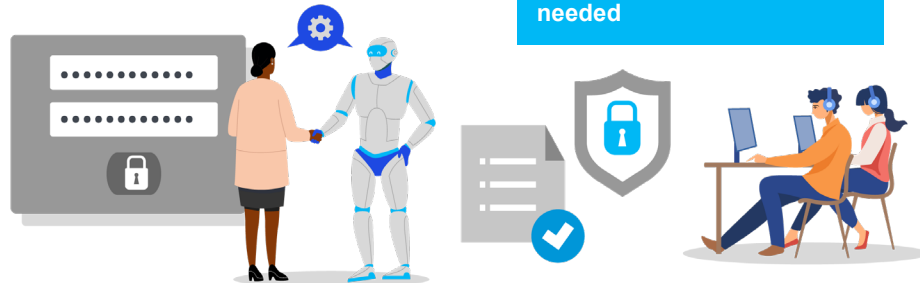
Latin America

330+

Asia Pacific

520+

Member firms located in key markets around the world that can be leveraged where needed



Certifications for specialised incident response work

We hold a number of accreditations for our lab that we use for cyber investigation and response purposes:

- Cyber Essentials Plus
- ISO/IEC 17025:2017 certified
- KPMG certificates: ISO27001:2013 certified
- Accredited National Cyber Security Center (NCSC) testing lab
- Accredited by CREST and NCSC.

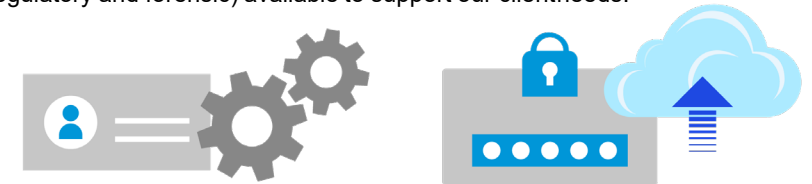
Our incident response approach is aligned with major IR standards such as NIST SP800-86 and ISO 18044:2004

Flying squads

For regions where KPMG does not have a presence, our 'Flying Squad' model allows us to effectively put boots on the ground within 24-48 hours, moving staff across borders to meet our client needs.

Our global capabilities

KPMG has over 3,000 professionals dedicated to delivering Cyber Security services around the world, with over 25,000+ additional risk-focused consultants (with a variety of backgrounds – including IT, regulatory and forensic) available to support our client needs.



Our Services

Despite efforts to maintain tight security across the networks and systems, cyber-attacks remain inevitable. This means there's a strong business case for embedding a proactive cyber security strategy and effective response capabilities.

Prepare

Ensuring your organisation is fully prepared in the event of a cyber attack.



Cyber Incident Playbook development

We can assist with the creation and development of technical playbooks on a per application, technology, or scenario basis by:

- Advising on leading practices and industry standards
- Providing standardised templates
- Maintaining an open dialogue to support with playbook development
- Ensuring all company decisions regarding response plans and playbooks are documented



Incident Readiness Review

We can engage with the business and stakeholders to perform simulated attacks which help to assess how well the business handles and responds to an incident, as well as identify any skill or performance gaps that need addressing.



Training and Awareness support

We can assist with the training and awareness of your response and recovery plans by:

- Performing interactive simultaneous multi-team testing and war games to harden defenses
- Supporting with the creation of standard and role based training materials for response and recovery to ensure incident response is understood by all.

Respond

Providing an expert incident response service to help safeguard your IT and OT assets during and after an attack.



Attack Disruption

Our team of experts will work swiftly to identify the root cause of the cyber-attack, contain the attack itself, and remediate it. They will ensure that any access an attacker may still hold on your systems, networks or services is identified and disrupted quickly to avoid any further damage.



Threat hunting

Our team of threat hunters will monitor your network to ensure that recovery teams safely recover your systems and bring your services back to usual business operations.



Digital Forensic Investigation

KPMG has a dedicated Forensic Technology lab which enables the recovery and use of critical digital evidence to support investigations and litigation.



Threat Intelligence

Threat Intelligence Service complements your organisation's cyber response by providing actionable, relevant and timely information about the attack. In addition to researching threat actor campaigns, monitoring brands, credential leakage, and supply chain threats, it includes insights into operational and strategic decisions.

Recover and Beyond

Supporting the fast recovery and restoration of your systems and services, and helping to identify key improvement areas to your cyber capability through lessons learned.



Crisis Management

For significant breaches affecting multiple regions, we will setup a crisis management office that will coordinate with bronze, silver and gold committees for driving the recovery of systems and services across each region..



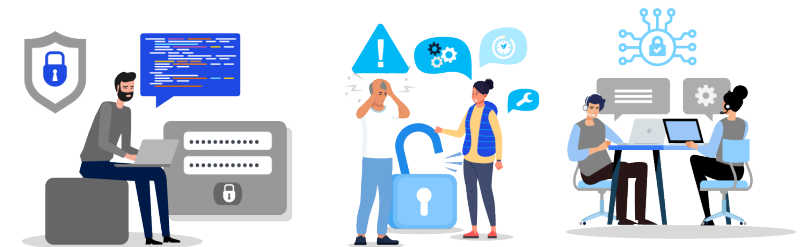
Restoring Business and Technology Services

We understand that in case of an incident you may lose access to your servers and data thereby affecting your services to wider business. We will assemble a team of infrastructure, cloud and data architects who will help you recover your business services.

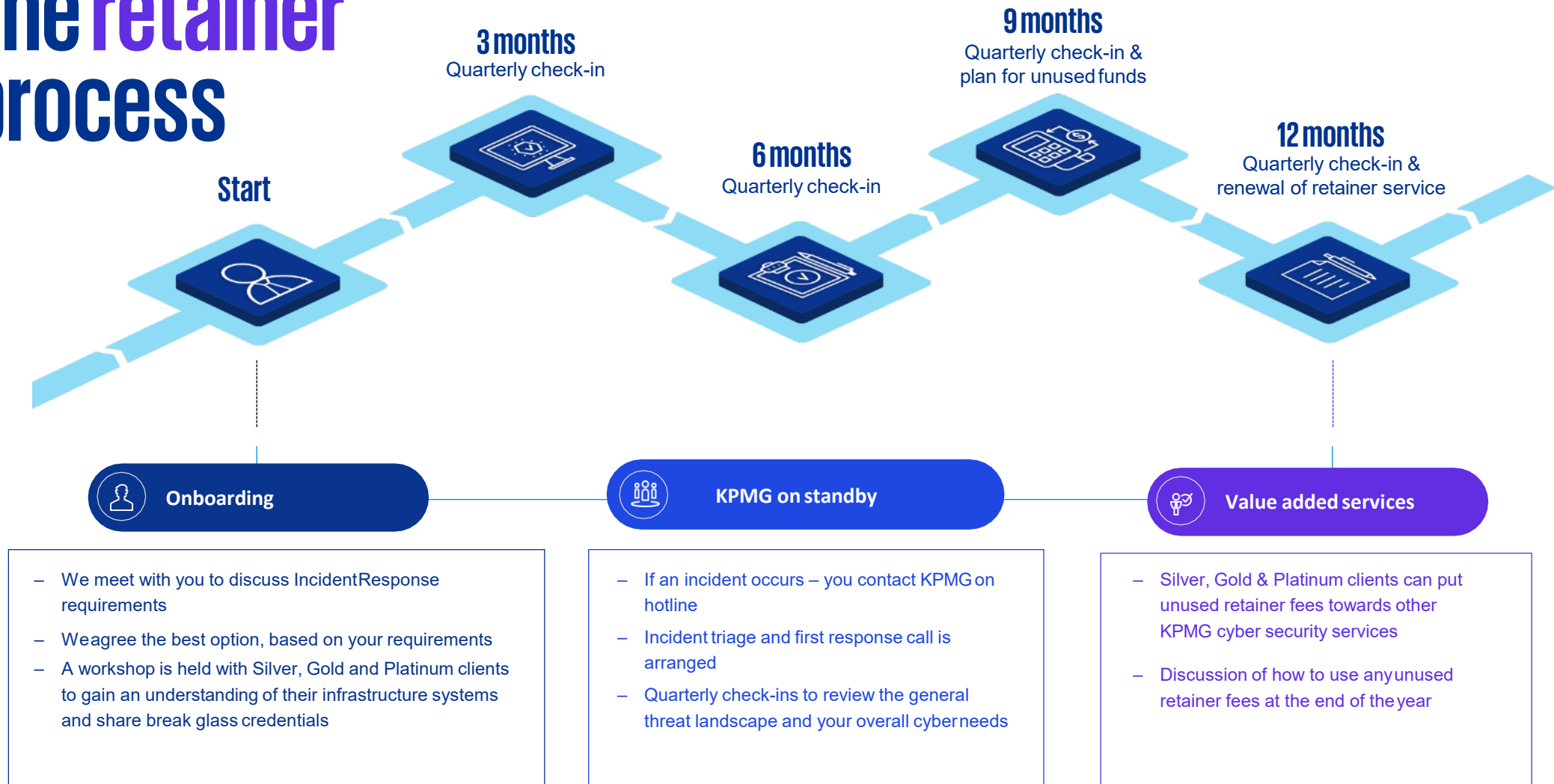


Legal and eDiscovery

Our team of eDiscovery specialists will build a clear picture of data and subjects affected by the breach which will help you notify regulators and customers in the most informed way.






The retainer process



Support levels

We offer different support levels to ensure we meet your incident response requirements.

	 Silver	 Gold	 Platinum
Annual pre-payment:	£35k	£70k	£115k
Number of hours^(a)	80	180	350
Callout fee:	POA	POA	None
Onboarding and security workshop^(b):	Standard security workshop	In-depth security workshop	Bespoke
24/7 incident notification hotline	✓	✓	✓
First response^(c):	8 hours	4 hours	2 hours
Coverage and on-site response within SLA^(d):	Next business day at 3 pre-agreed locations in the UK and Europe	24 hours at 3 pre-agreed global locations	Bespoke (anywhere globally)
Use the remaining retainer on other cyber security services^(e)	✓	✓	✓

Notes

- a) Estimated number of hours based on blended team.
- b) Please see the "What's in the onboarding and workshop?" page.
- c) Time from the initial notification by client (you) until a KPMG incident triage call with a specialist KPMG incident manager.
- d) SLA time from completion of the triage call. KPMG will perform commercially reasonable endeavours to provide remote assistance sooner, but within the on-site service level agreement window. Location will be agreed at the contracting time.
- e) Clients can use their retainer hours for any other consulting engagements that includes but not limited to purple team exercise, threat hunting, SOC maturity assessment, etc. These services can be discussed and agreed on 3rd quarterly check-in meeting.

What's in the onboarding and workshop

Why onboarding and workshop are important?

Before an incident occurs, it is wise to become familiar with each other. We will be more efficient if we get to know each other better which is why onboarding workshops are critical for the success of retainer programs. We will discuss your security architecture and processes during the initial onboarding and agree on general working methods.

Together, we will explore common incident response situations to identify how to respond to them and if there are any problems that might arise.

The type of onboarding and workshop depends on the service level you have selected:

01



Basic onboarding

- One hour meeting at KPMG's offices or a conference call involving you and the appropriate business stakeholders.
- Exchange of key contact information.
- Exchange of break glass credentials
- Network, system and application environment overview.
- Review of the questionnaire and follow on discussion with wider team on answers provided in the questionnaire.
- High level security recommendations gathered from the onboarding meeting.

02



In-Depth security workshop (single day)

- Three hour workshop at your chosen location including yourselves and members of KPMG's incident response team.
- Exchange of key contact information.
- Exchange of break glass credentials
- Review of the questionnaire and follow on discussion with wider team on answers provided in the questionnaire.
- One standard incident scenario walkthrough (table-top exercise) testing your current crisis management processes.
- Review of current security documentation including current incident response plan, communications plan and past cyber incident reports.
- Security control recommendations based upon the knowledge we've gathered from the workshop on your current incident response vulnerabilities.

Related services for unused funds



Threat hunting

- A proactive defence activity focused on:
- Network discovery
- Malware detection
- Attacker analysis
- Persistent risk investigation



Penetration testing

- A simulated attack on an environment varying from:
- Application testing
- Network testing
- Infrastructure examinations
- Vulnerability assessment



Purple teaming & war gaming

- A collaborative cyber exercise engaging your red and blue teams for a live simulated attack that:
- Covers technical and non-technical spheres
- Splits attack and defence between two technical teams
- Aids preparation for an attack
- Helps to determine security posture



Table top exercise

- A discussion exercise for emergency situations helping to refine:
- Crisis management processes
- Incident response readiness
- Crisis communications
- Gaps in current proceedings



Cyber Risk Insights

- Capture and tracking of inputs needed to identify and quantify cyber risks
- Graphical modelling of a range of cyber-risk scenarios, using a defence-in-depth approach
- Measure cyber-risk exposure and potential losses in financial terms
- Evaluate the effectiveness of cyber capabilities against three key components: process maturity, technical effectiveness and coverage
- Providing clear, graphical information to support strategic cyber risk management decision-making
- Industry benchmarking



4Di

- Conduct threat level cyber incident response exercises tailored to your organisation
- Threat modelling and cyber intelligence to develop realistic simulated attacks
- Bespoke exercises can be developed rapidly, reducing lead times Reduced costs from
- - Suitable for team and individual development, with the ability to generate individual, participant-level metrics instantly

Why Obtain an IR Provider?

Higher Education has recently been determined as the most likely educational body to become a target for cyber attacks (TimesHigherEducation Survey 2023). With UK Higher Education extending to have global footprints In terms of partnering institutions, having an IR service provider who also have global reach will greatly benefit to protect staff and student data in the event of an attack.

Reasons incidents may occur

University Ways of Working:

Universities encourage the free flow of information and ideas, mobile working, BYOD and have an ever evolving student and faculty population. This is causing an increase in both Cyber Security and business risks across the board due to a lack of Cyber Security controls in place.

Information Security Budgets:

People, processes and technologies are required to deliver a Cyber Security capability. Without adequate budgets the Cyber risk landscape remains unmitigated and Universities continue to be exposed.

Malicious Attacks (e.g. Phishing):

Threat actors are actively targeting student and faculty accounts across all Universities. Researchers, notable students and individuals with financial authority are all example targets.

Logging and Monitoring:

Having visibility over devices connecting to the network and being able to monitor user activity (authorised and unauthorised). Therefore there is a risk that threat actors remain undetected.

Unmanaged Devices:

Unmanaged devices is a challenge that universities recognise. A single university have around 40,000 unmanaged devices touching the network at any one time with no visibility or control over the data that they're accessing and storing.

Motive



Financially Motivated



Corporate Espionage



Malicious Insider



Political / Social Hacktivist

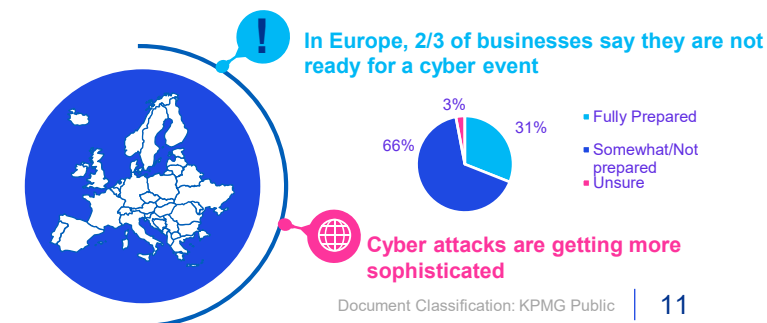


Negligent Insider



State Sponsor

Current state of preparation



News Coverage

As cyber attacks continue to become more prevalent and cyber threat actors increase in technical proficiency. We at KPMG feel it is our responsibility to keep up to date with the latest trends within the threat landscape.

In particular we like to look into relevant coverage for our clients. To the right there are some of the latest or biggest cyber attacks involving Higher Education.

Irish Independent 

Irish university confirms data posted on darkweb after cyber attack.

Published: 12th February 2023



University of Manchester hit by cyber attack.

Published: 9th June 2023

**CRAIN'S
CHICAGO
BUSINESS**

Loyola among colleges warned of data exposure from MOVEit hack.

Published: 20th July 2023



CYBER BREACH Urgent warning as hackers put thousands of students' details on dark web.

Published: 13th August 2023

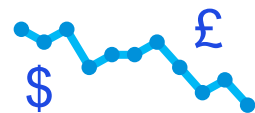
BLEEPINGCOMPUTER

University of Michigan shuts down network after cyberattack.

Published: 29th August 2023

Cyber Attack Impact

The threat landscape is constantly changing, especially when broken down to sector specifics. With cyber threat actors upskilling in their areas of expertise it is important to look to the significant impacts they can level their attacks to. This is so we can remain aware of how our client's crown jewels may be attacked and what may be targeted. The following are impacts that tend to affect the Higher Education.



Loss of Contracts / Funding

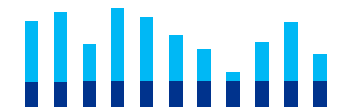
Government and commercial contracts are increasingly requiring Universities to have Cyber Security certifications and capabilities. Without these, Universities may lose out on current and future revenue and research opportunities.



Reputational Damage

Universities rely heavily on the reputation and trust that they uphold. The multi-faceted and varied nature of Cyber attacks means that reputation and trust can quickly be lost, as seen in the commercial space.

Financial Impact



A London based University was the first to be fined by the ICO due to a “serious” data breach involving student and staff records. This resulted in a fine of over £100,000 for not having implemented adequate technical and organisational measures.



Operational Impact

A number of operational impacts to a University can arise from Cyber Security risks materialising. For example;

The ICO could force Universities to stop their data processing activities as a result of a breach. During certain times of the year such as clearing, the impact would be substantial.