RHICS IT
MANAGEMENT CONSULTANCY

CYBER RESILIENCE PROGRAMME

www.rhics.io

ABOUT THE PROGRAMME

With the increasing sophistication of cyber threats, businesses are facing significant risks of cyber attacks such as data breaches, ransomware attacks, and phishing scams. These attacks can cause financial losses, regulatory fines, and damage to your business reputation.

At Rhics Technology, we specialize in providing tailored cybersecurity solutions to help your business strengthen its cyber defenses and protect your members' data. Our team of cybersecurity experts understands the unique challenges faced by businesses and offers customized solutions to address them.

We believe that cybersecurity is not just an option, but a necessity in today's digital age. As technology advances, cybercriminals continue to find new ways to exploit vulnerabilities in IT systems and infrastructure. To ensure the safety and security of your members' data and your business reputation, it's crucial to have a comprehensive cybersecurity strategy in place.

We take pride in offering the latest and most effective cybersecurity solutions to help protect your business and members. Our services include cybersecurity assessment, vulnerability scanning, penetration testing, and risk management. We work closely with our clients to understand their unique needs and provide them with customized solutions to address potential vulnerabilities.

In conclusion, at Rhics Technology, we are committed to providing businesses with top-tier cybersecurity solutions to safeguard their business's and members' data.

Don't wait until it's too late, contact us today to schedule a cybersecurity audit for your business and ensure your cybersecurity strategy is up-to-date and effective.

CYBER THREATS ON CREDIT UNIONS

Businesses hold sensitive information such as members' personal and financial data, making them a prime target for cybercriminals. With the increasing sophistication of cyber threats, businesses face significant risks of cyber attacks such as data breaches, ransomware attacks, and phishing scams. These attacks can cause financial losses, regulatory fines, and damage to your credit union's reputation.

COMPREHENSIVE CYBERSECURITY STRATEGY

To safeguard your business and your members' data, it's vital to have a comprehensive cybersecurity strategy in place. Rhics Technology offers tailored cybersecurity solutions that address your unique challenges. Our team of cybersecurity experts will work with you to identify potential vulnerabilities and implement measures to prevent cyber attacks.

IMPORTANCE OF CYBERSECURITY AUDIT

One of the most crucial steps in strengthening your cybersecurity defenses is to conduct a cybersecurity audit. Our audit process is thorough and will identify any weaknesses in your credit union's IT systems and infrastructure. Here are some reasons why a cybersecurity audit is critical for your credit union:

- Identify vulnerabilities: A cybersecurity audit will help you identify any weaknesses in your current security systems and protocols.
- Stay compliant: Businesses like financial institutions are required to follow specific regulations and guidelines. A cybersecurity audit will ensure that you are meeting these requirements.
- Protect your reputation: A cyber attack can damage your business reputation and erode your members' trust. A cybersecurity audit can help you prevent this from happening.

THE BENEFITS OF A CYBERSECURITY AUDIT

There are many benefits to having a cybersecurity audit. Some of the most important benefits include:

- Identifying vulnerabilities and weaknesses in your systems and networks
- Assessing your overall security posture
- Identifying areas where you need to improve
- Complying with regulatory requirements
- Reducing the risk of a data breach
- Protecting your organization's reputation
- Reducing the cost of a data breach

If you're not sure whether or not you need a cybersecurity audit, the answer is probably yes. Even if you think your organization is secure, it's important to have an expert take a look at your systems and networks to identify any potential vulnerabilities. A cybersecurity audit can give you peace of mind knowing that your organization is doing everything it can to protect itself from cyber attacks.

PROGRAM STRUCTURE

The cyber resilience program (CRP) is a program designed to help businesses understand, manage, mitigate, and respond to digital and cybersecurity threats in real time. It will equip businesses with skills and competencies that may not be available in-house. The program is broken down into 3 key areas.

RISK ASSESSMENT

- Business Process Analysis
- Regulatory Compliance Review
- Business Products & Service Reviews
- Digital / Mobile Banking Platform Review
- Risk Assessment matrix
- Recommend Risk Assessment Framework Identify & Highlight Risks
- In-house IT Competency Review Penetration Testing / Ethical Hacking

RISK MITIGATION

- Risk management Regime
- Policy document review
- Policy document recommendations
- Recommend RegTech solutions for onboarding, eKYC, SCA, transaction monitoring et al (Requires partnership with suppliers)

INCIDENT RESPONSE

Turnkey Cyber Security incident response plan customized to incident type.

WHY CHOOSE RHICS FOR YOUR CYBER SECURITY AUDIT

Firstly, our team of experienced cyber security professionals has a deep understanding of the latest threats, vulnerabilities and risks facing organizations of all sizes. We use a proven methodology to assess your systems, processes and procedures and provide a comprehensive report detailing our findings and recommendations.

Secondly, our customized cyber security audit services are tailored to meet the specific needs of your organization. We work closely with you to understand your business goals, operations, and technology infrastructure to develop an assessment that provides the most value and insight.

Thirdly, we offer a range of training programs that can help educate your employees on the latest cyber threats and best practices. Our training programs are designed to be engaging and interactive, helping your employees understand the importance of cybersecurity and how to identify and mitigate potential threats.

Finally, at Rhics, we are committed to providing exceptional customer service and support. We work closely with you throughout the entire process, from initial assessment to implementation of recommendations, to ensure that you have the support and guidance you need to protect your organization from cyber threats.

In short, Rhics is the ideal partner for your cyber security audit and training needs, providing a comprehensive, customized approach that delivers results and peace of mind.

WHAT TO EXPECT FROM A CYBER SECURITY AUDIT LED BY RHICS

A Rhics cybersecurity audit typically involves the following steps:

Planning: The first step is to plan the audit. This involves identifying the scope of the audit, the resources that will be needed, and the timeline for the audit.

Data gathering: The next step is to gather data about the organization's systems and networks. This data can be gathered from a variety of sources, such as network logs, security devices, and employee interviews.

Analysis: The data that is gathered is then analyzed to identify vulnerabilities and weaknesses.

Reporting: The results of the audit are then reported to the organization. The report will include a description of the vulnerabilities and weaknesses that were identified, as well as recommendations for how to fix them.

Implementation: The final step is to implement the recommendations that were made in the audit report. This will help to improve the organization's security posture and reduce the risk of a data breach.

REAL-LIFE CASE STUDY OF CYBER ATTACKS ON BUSINESSES DATA

According to a report by the Credit Union National Association (CUNA), cyber attacks targeting financial institutions like credit unions have been on the rise in recent years. In 2020, 37% of credit unions reported being victims of a cyber attack, up from 20% in 2018. The report also found that the average cost of a cyber attack for credit unions was $17,000, with some attacks costing more than $1 million in damages. These statistics highlight the importance of cyber security measures for businesses to protect their members' personal and financial information.

There have been several cyber attacks targeting financial institutions in recent years. Here are some real-life examples:

CYBER ATTACKS ON FINANCIAL INSTITUTIONS

Almost two-thirds (65%) of large financial services companies have suffered a cyber-attack in the past year, while 45% have experienced a rise in attack attempts since the start of the COVID-19 pandemic.

CASH APP

The attack on Cash App, a payment tool, in 2022, did not come from a previously unknown digital vulnerability or a cybercrime campaign. Rather, this data breach involved a former employee who accessed the company's servers, took records containing customer's personal information including names and account numbers, and shared them.

The attack compromised the names, trading information, and stock portfolios of 8 million users. This information could allow digital crime organizations to access user bank accounts, conduct identity theft, and gain entry to social media accounts.

MORGAN STANLEY

In 2015, Morgan Stanley, one of the largest financial service companies in the world, was forced to pay a $1M penalty for failing to protect their customers' records. This was after the company lost $730,000 in customer records to hackers and 6 million account records of Morgan Stanley clients were being offered up for purchase.

CYBER ATTACKS ON BUSINESSES

Small businesses account for 43% of cyber attacks annually and 46% of cyber attacks were small businesses with 1,000 or fewer employees. Only 14% of these SMBs are prepared to face such an attack. On average, small and medium-sized businesses (SMBs) lose $25,000 due to cyber attacks. The next five years are due to see a 15% increase in cybercrime costs reaching 10.5 trillion by 2025.

ADVANCED ELECTRICAL VARNISHES LTD (AEV)

AEV is a Wirral-based manufacturing firm, it suffered a malware cyber breach. The financial controller unknowingly exposed the full pin of the company's banking account. Just 3 minutes later, $30,000 had been sent to an account in Ukraine and €100,000 to another in Cyprus. The unsettling thing is that this happened so fast and it could have happened to anybody, any employee, any company.

FATFACE

In 2021, the Conti gang successfully attacked the fashion retailer, FatFace, network via a phishing attack on 10 January, a ransomware attack on 17 January, and more than 200GB of data was exfiltrated. The ransomware operators demanded a ransom of $8m but were successfully talked down during a protracted negotiation process and paid a $2m ransom to the Conti ransomware gang.

Seen enough?

These evidence-based examples show that security is a culture that modern businesses need to embrace completely because attackers constantly improve their techniques to find innovative ways into systems. Logically, we must constantly improve our techniques to keep them out.

The bottom line is, it doesn't matter how long you've been in business or how big your company is, cyber crime attacks are on the rise. The best thing you can do for yourself is to get a cyber security audit that can help your company prevent cyber attacks on your devices, employees, and servers.

Get our proven and trusted cyber security audit and regain peace of mind amidst cyber threats.

WHO WE ARE

Rhics is a creative digital agency headquartered in London, UK with branches across 4 continents. We specialize in Digital Strategy, IT Consultancy, Cyber Risk Management, Digital Marketing, Social Media Management, Mobile & Web Application Development, Design & Branding.

We have a proven history of creating online success for global organizations via our suite of services offerings. We help **define your goals, create effective strategies, build easy-to-use applications**, and design award-winning systems that communicate the desired message.

Our process unites talent & passion with discipline.

We are committed to providing affordable Digital Transformation education to the world.

RHICS IT
MANAGEMENT CONSULTANCY

CONTACTS

Email: info@rhicstech.com

United Kingdom
+44 7759 301221

Trinidad
+44 7747 677940

Nigeria
+234 805 579 3803

United Kingdom
RHICS Technology HQ
RHICS LTD, Kemp House, 152 - 160 City Road, London
EC1V 2NX

CLIENT WE HAVE WORKED FOR

www.rhics.io