Shelter from the Storm

RANSOMWARE READINESS AUDIT

Identify, protect, detect, respond & recover from a ransomware attack

4,000 / day

More than 4,000 ransomware attacks are launched each day.

$233K / £3.7M

The average ransomware payment is $233,217.00, approximately £164,413.32.

19 days

The average downtime after a ransomware attack is 19 days.

WannaCry

In 2017, the WannaCry ransomware outages accounted for a large number of security breaches and some responding organisations fell victim to the Locky and Zepto variants, with the most severe attack knocking systems offline for two weeks.

RANSOMWARE 101

Ransomware is a form of malicious software (malware) programmed to encrypt data on the system it infects rendering it inaccessible to its users. Threat actors then demand a ransom payment in exchange for the decryption key needed to unlock (decrypt) the data. It can be delivered through several different attack vectors and needless to say, it can have a significant impact on the business by denying it access to the data it needs to do business.

Whilst it has been around for a while, ransomware has greatly evolved over the last several years becoming far more sophisticated, easier to use and accessible to less skilled threat actors, and more prevalent on the threat landscape. The financial and reputational impacts of a ransomware attack can be significant so the risk should be treated accordingly.

What you may not have known is the risk of ransomware can be greatly reduced by simply implementing and adhering to some basic risk management principles and processes. So, the best way to protect your business from ransomware is to prevent it from happening in the first place and be ready for it if it does occur. Risk Crew can ensure both.

FIVE COMPONENTS

This service is based on simple practices – that actually work – and includes simulated ransomware attacks to test your real-world response capability.

1 Identify

Risk Crew begin by confirming your business' critical information assets to identify, specifically, where a ransomware attack could most harm the business.

We then map your existing security controls to these assets to verify coverage and detect gaps in protection. This confirms that your current controls are aligned to your most critical assets. Finally, we survey and benchmark the business' current level of awareness of the threat of ransomware, and potential entry points into the business.

This confirms that the business truly understands the threat and its consequences.

2 Protect

Next, we assess the effectiveness of your existing controls and processes implemented to mitigate an actual ransomware attack.
In this phase, we conduct ten different simulated ransomware infection attacks to evaluate your business' current controls against real-world threat attack scenarios.

This ensures that your current controls are fit for purpose.

3 Detect

After running false ransomware infections, we then assess how quickly the system and users detect the simulated attacks and report them to the appropriate business division or point of contact.

We assess anti-malware security software and hardware products for their ability to identify and quarantine the bogus infections.

This confirms how quickly your business can identify an attack.

4 Respond

Next, we assess the business' response to the simulated ransomware attacks. This is done through a table-top walk-through of the existing Incident Response Plan and monitoring the actual "live" exercise".

We assess staff for their execution of these plans as well as their professional skills and experience in mitigating ransomware attacks.

This confirms that the business has the capability to appropriately respond to a ransomware attack.

5 Recover

Finally, Risk Crew audit the business' capability to recover from the simulated ransomware attacks. This is done through table-top walkthroughs of the existing Business Continuity and Disaster Recovery (BC/DR) plans to confirm their applicability to conditions resulting from the "live" exercise.

We verify the system back-ups and assess documented business impact assessments (BIAs) for their relevance and accuracy. Evaluation of BC/DR vendor solutions are done for efficiency and effectiveness in this final phase.

This quantifies the business' actual capability to recover from an attack – quickly and thoroughly.

SIMPLE & EFFECTIVE

This service ENSURES that you are prepared for the worst by testing your business' "READINESS" for a ransomware attack and its ability to recover from one – in the event that it fails.

THE BENEFITS

The service results in a comprehensive report detailing your business' capability to identify, minimise and manage the risk of a ransomware attack along with cost-effective recommendations for significantly improving your defensive capability.

Our Ransomware Readiness Audit also provides these tangible business benefits:

- Significantly reduces the likelihood of a ransomware attack disrupting your business operations
- Minimises business disruption in the event of an attack reducing downtime
- Mitigates regulatory, compliance and reputation impacts resulting from an attack
- Improves current security readiness policies and procedures
- Reduces cyber-insurance costs

Is your business ready for a ransomware attack? Knowing the answer is the biggest benefit.

WHY CHOOSE RISK CREW?

Risk Crew security consultants possess over 30 years of hands-on skills and experience in malware, and designing and testing incident response, business continuity and disaster recovery plans. It's what we do. We: think deeply, question assumptions, determine cause and effect and always deliver measurable results.

We like to help. It's what we do.

WHAT OUR CUSTOMER'S SAY

"I have dealt with Risk Crew for several years. Their professionalism and attention to detail are second to none and they have a comprehensive and extensive knowledge of all the relevant standards and regulations. They are able to present complex solutions so that they can be understood by staff at all levels. Their training modules are excellent. I would recommend using Risk Crew."

Technology Industry Customer

"Once again, Risk Crew impressed our Board (and made me look like a star). Well done."

Security Industry Customer

"A very positive experience. Risk Crew staff were friendly and professional throughout the engagement, keeping me informed and addressing all concerns in a timely manner. I won't hesitate to recommend Risk Crew or use them for future engagements."

Utilities Industry Customer

"Wow! Simple and really effective. Something the whole business easily understood and could get behind."

Finance Industry Customer

"I highly recommend this team of very knowledgeable people. They are excellent professionals at the service of their customers. The team know RISK MANAGEMENT (in capitals) and they always deliver. "

Medical Industry Customer

Dealing with ransomware just takes the right crew – the Risk Crew.

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234

riskcrew.com

info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom

risk crew

Shelter from the Storm