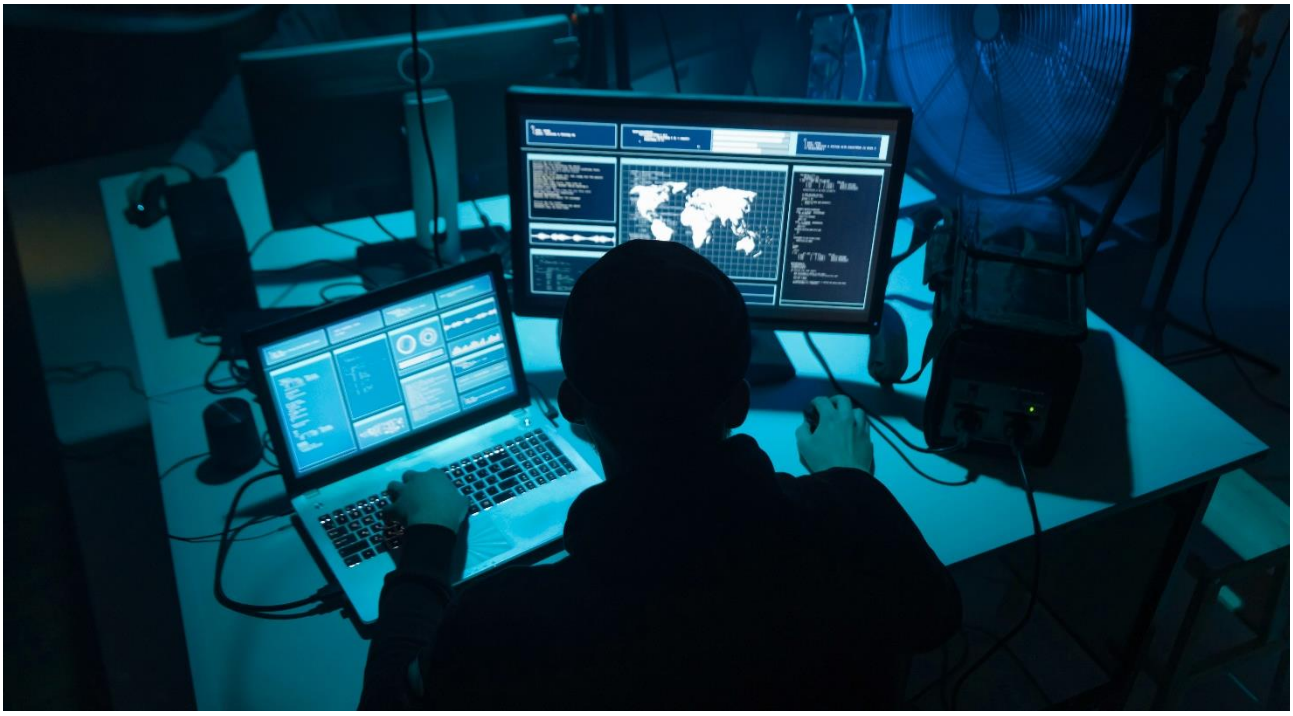
Organisational Resilience: Ransomware

Developing a Response Strategy



Ransomware attacks pose a serious cyber threat to organisations by preventing access to data with the subsequent knock on effect of interruption to day to day business operations. This paper explores the key factors organisations should consider when developing a ransomware response strategy.

To pay or not to pay, is that the question?

As the societal dependency on IT and connected systems increases, we are collecting and producing a huge amount of data which has become the backbone of every business. Information is then produced by the interpretation of these data and all organisations in both the public and private sectors are directly reliant on this information for the day to day running of the business.

In our paper covering Phishing, we highlighted how cyber-criminals exfiltrate data from businesses to sell on the dark net. However, not all data has a value on the black market and cyber criminals need to find other ways to make money. Recognising that data has value to businesses, by making that data unavailable and stopping the manufacturer of products or delivery of services, the cyber-criminal can demand a sum of money in return for the restoration of data access. These types of malicious software which create unavailability of system or data are collectively known as Ransomware.

So, in these situations the big question for a business is “to pay or not to pay?”. In UK, the National Crime Agency recommendation is not to pay any demand, an approach fully supported by the National Cyber Security Centre, as this funds criminal activity, encourages further such activity and provides no guarantee that access will be restored. However, faced with a business interruption that could cost a business millions in lost revenue and additional operating costs choosing not to pay a ransom demand is not a simple easy answer.

Is cyber insurance the silver bullet?

Cyber insurance can help an organisation get back on its feet when things go wrong by providing financial protection against the impacts of a cyber event, such as business interruption costs as well as cover for ransom payments. Policies can also include support services that are useful during a security incident, such as IT forensics and legal assistance. However, insurance should always be considered as a safety net, providing protection for when things go wrong but not as a replacement for a coherent risk management approach. In other words, the organisation needs to properly understand what the impact of a cyber incident would be and the extent to which it is protected by means of technical and procedural controls, in particular the ability to restore systems and data in the event of a ransomware attack.

Do organisations actually pay?

Many organisations will not publicly disclose whether demands have been paid. However, research undertaken by IBM Security's X-Force indicates that a large percentage of businesses have paid the ransom to get their data back. One such case was Florida City who paid $600,000 in ransom to hackers in June 2019. The payment was covered by insurance though the FBI does not support paying of ransom.

Earlier this year a large financial services organization suffered a successful ransomware attack perpetrated by the cyber-criminal group REvil and eventually paid a ransom of just over £2.6m to restore their systems. However, they could not trade for over 90 days and with an annual turnover of around £1Bn the incident cost the business over £25m according to their quarterly report. In August 2020 the company has gone into administration, with the impact of the cyber-attack being quoted by the administrators as one of the key reasons for failure.

At around the same time a UK local authority suffered a similar ransomware attack. It has taken the Council four months to restore systems after a decision not to pay the ransom was made. It has not been reported whether all data that was encrypted has been successfully recovered. The current cost of recovery is estimated at £11m, almost 4% of the annual budget.

To Pay or Not to Pay, is not the right question

Considering the above cases, where some paid, some delayed and then paid and one never paid, the right questions to ask or consider are:

1. How confident are we in our disaster recovery capability?
2. When was the last time we tested that capability?
3. Do we have properly tested business continuity plans that are aligned with our disaster recovery arrangements?

Disaster Recovery not just backup

There's an important distinction between backup and disaster recovery. Backup is the process of making an extra copy (or multiple copies) of data. Disaster recovery on the other hand refers to the plan and processes for quickly re-establishing access to applications, data and IT resources after an outage.

Business resiliency – the ability to come back to life from an incident as quickly as possible with minimum disruption to internal and external stakeholders as well as reputation – needs a properly designed disaster recovery solution. Understanding digital assets, where they are stored, how they are processed, and which assets are most critical to the business is an important first step in this process and one which will guide the choice of recovery strategies. This Business Impact Assessment will guide the design of arrangements so that in case of a disruptive incident, recovery or failover action will prioritise the systems and data that support the critical parts of the business.

Many businesses are now turning to external suppliers for complete disaster recovery solutions and moving away from traditional on-premises replication of infrastructure, systems and data. Disaster Recovery as a Service (DRaaS) offers several benefits including lower costs, enhanced reliability, speed of recovery and improved administration. However not all DRaaS offerings are created equal and a clear schedule of requirements that reflect business needs and priorities should be drawn up before approaching any potential supplier. The following points should also be considered:

- Ensure the supplier meets industry security standards and territorial privacy regulatory requirements.
- Verify that your data is encrypted at rest and in-transit.
- Understand how the supplier authenticates users from the virtual failover environment
- Select a supplier that offers contractual Recovery Time Objectives (RTO) and Recovery Point Objectives (RTO).
- Understand the extent of testing the supplier performs to ensure recovery within the prescribed timeframes.

Whilst Disaster Recovery provides a technical response to disruptive incidents it is critical the arrangements link seamlessly with enterprise wide business continuity plans. This will ensure a coherent response across the business, enhancing decision making and resource allocation. It will also make certain that stakeholder management is integral to response and recovery efforts. As with disaster recovery arrangements, business continuity plans should be exercised to validate their suitability and effectiveness.

What else to consider in the fight against Ransomware?

Just having the post-breach ability to recover from disaster using backup is not enough as a mitigation for a ransomware event. Other things to consider as a pre-breach mitigation as well as to reduce the surface of the attack are:

1. Prevent malware delivery and execution. This is a combination of up to date malware protection along with web filtering and email filtering.
2. Apply network and system hardening as well as permitting only the execution of trusted applications from trusted sources.
3. Run up to date operating system and software products and apply critical security updates as soon as available. Apply network segregation and other compensating controls for running old and unsupported platforms.
4. Deploy good authentication practices including Privileged Access Management, Good Password Policy and the use of MFA (Multi-factor authentication). Prevent unwanted internet and email access to all network admin accounts.
5. Develop an Incident Response Plan and playbook for ransomware and exercise at regular intervals with table-top exercises. Identify the specialist technical resources, such as digital forensics, that may need to be "bought in" as part of the response.

Summary

Whatever an organisations decision is on the "to pay or not to pay" the position should be pre-agreed by the senior management team to avoid the decision having to made under the stress and duress of a live cyber-attack. For all organisations there is a balance between weighing up the financial costs of a ransomware attack versus paying a ransom to quickly restore systems and data. However, this isn't just a financial balance, it's also a moral balance and in some sectors a regulatory issue.

Protection against ransomware needs a rounded approach. Proportionate controls should be applied to protect systems and detect security events. Plans need to be drawn up that set out how the organisation will respond to such an event, both from a technical IT perspective and the continuity of business-critical services and activities.

As cyber criminals continue to enhance their attack methods so must organisations continually review their cyber risk posture to ensure they are adequately protected and prepared. At Zurich our Cyber Risk Engineers can support organisations with risk identification and mitigation helping develop organisational resilience.

Zurich Insurance plc, a public limited company incorporated in Ireland. Registration No. 13460.Registered Office: Zurich House, Ballsbridge Park, Dublin 4, Ireland. UK Branch registered in England and Wales Registration No. BR7985. UK Branch Head Office: The Zurich Centre, 3000 Parkway, Whiteley, Fareham, Hampshire PO15 7JZ.

Zurich Insurance plc is authorised by the Central Bank of Ireland and authorised and subject to limited regulation by the Financial Conduct Authority. Details about the extent of our authorisation by the Financial Conduct Authority are available from us on request. Our FCA Firm Reference Number is 203093.