

mimecast

KONCISE SOLUTIONS

CONNECTING THE DOTS

To Pay or Not To Pay:

ransomware has become
boards' biggest concern

Executive panel calls for better transparency,
more government engagement

Corporate boards, cybersecurity professionals, insurance companies and government bodies are all reviewing their security policies and risk-management procedures. This is according to a panel of security professionals who all report widespread concern over the increasing frequency of ransomware and nation-state attacks.

Government advice is to not pay ransomware criminals, and improved data backup procedures have made restoring encrypted data easier than ever. Yet, many of the attendees at Mimecast's latest Cyber Resilience Executive Society Roundtable (CRES) said their companies are still weighing the benefits of a payment, to avoid having data leaked in increasingly common 'double extortion' attacks.

In double extortion attacks, malicious code quietly exfiltrates as much corporate data as possible, sending it back to its authors before the ransomware encryption begins. This gives cybercriminals more leverage as they pressure companies to pay up or risk having sensitive data and corporate secrets made public.

After a recent spate of high-profile ransomware attacks that resulted in the payment of a ransom – including Colonial Pipeline (which paid \$US4.4m to cybercriminals)– attendees said conversations about ransomware strategies are dominating boards' risk discussions. One participant called ransomware "the biggest concern in our board meeting" and noted that the subject "occupied 75% of the discussion."

Moderator David Barlett – a former premier of Tasmania who went on to lead companies and people across all sectors as a non-executive director and chairman, keynote speaker, and digital futures advisor – offered a view from the top, where risk-averse boards are discussing business resilience like never before.

Common topics of concern, he said, include:

- **a company's ability to detect and respond to attacks**
- **whether to pay a ransom or not**
- **how to settle on a broadly acceptable ransomware response policy**
- **reporting obligations to APRA and other statutory bodies, including who receives notifications; when; and what follow-up action needs to be taken**
- **desktop exercises to get everybody on the same page**
- **how to resolve differences of opinion between the C-suite and board.**

Among companies that have already been hit by ransomware, a key concern is making sure that it doesn't happen again. This includes training staff to prevent them falling victim to attacks, and by implementing better technological protections to detect and block ransomware attacks while they are happening.

Among companies that have already been hit by ransomware, a key concern is making sure that it doesn't happen again. This includes training staff to prevent them falling victim to attacks, and by implementing better technological protections to detect and block ransomware attacks while they are happening.

Weighing board obligations

Some attendees raised questions about whether board members have an ethical duty to disclose having paid or not paid a ransom – an issue that has become particularly timely given recent Australian government **discussions** about a potential mandatory ransomware payment reporting regime.

Such disclosure was acknowledged by some panel members as being important to the protection of the corporate brand, while others felt it was within the normal duties of a director.

Still others wondered whether a higher degree of disclosure would lead to board members being held accountable for not mitigating risk around ransomware.

“In cyber scenarios, the board does not want to make the hard call” when ransomware strikes, one delegate said, advising others to “have a conversation with general counsel well before time”. Companies should have a clear plan to either get their data back, or to pay so that data is not disclosed.

Most companies don’t have an explicit policy that says they can’t pay ransomware, another CRES participant noted, adding that “it comes down to circumstances and situation”.


“Time is against us,” the participant said, advising security professionals to actively research ransomware groups to find out whether they have a history of honouring non-disclosure payments.

Others pointed out the role of insurance companies, with one attendee reporting that the insurance company had pressured them to pay, “as it is the quickest and easiest way to get back to business”.


Ransomware criminals rely on insurance companies to pay companies’ ransoms, for this attack method to remain lucrative. In response some insurance companies are starting to refuse to pay ransoms on the basis that customers need to be more proactive at protecting themselves.

“Insurance companies need to stop paying ransoms,” one panel member said, noting that they are often paying higher ransoms because cybercriminals feel they have deep pockets.

“This is funding the [ransomware] industry and funding the capability to launch future attacks,” the attendee observed.



Ransomware criminals rely on insurance companies to pay companies’ ransoms, for this attack method to remain lucrative. In response some insurance companies are starting to refuse to pay ransoms on the basis that customers need to be more proactive at protecting themselves.



Outside Threats, Outside Support

Another growing area of concern – highlighted by the Colonial Pipeline breach’s impact on real-world petrol supply chains – is the increasing vulnerability of operational technology (OT) networks. These typically sit outside the protection of information technology (IT) networks and are proving to be an Achilles’ heel for companies working to reduce their security exposure.

Some attendees have implemented a physical ‘air gap’ between corporate networks and control networks. While many worry that OT exposure is becoming a vector for exploitation by cybercriminals. Even more concerning are the nation-state actors who are aiming for maximum disruption and may have non-financial motives that can’t be resolved with a simple payoff.

Security staff have become better at patching the vulnerabilities that are being exploited by nation-state actors, attendees said, but a “substantial increase” in activity by hostile foreign governments is proving problematic. “We have very low levels of capability and preparedness in Australia,” one panel member observed. “Spy agencies might be doing some good work and recruiting a lot of talent, but there will always be weaknesses.”

That ever-present risk means that companies should stop trying to take the easy way out by paying ransoms, another member said, advising that the only time to pay is when it has created an “existential threat” – as happened when Colonial Pipeline interrupted fuel supplies to tens of millions of people.

“Otherwise, do the hard yards to recover,” one participant said.


Australian government involvement is a weak point in corporate ransomware response, with one panel member saying the government “needs to make a big leap in terms of communications” about ransomware risks and viable remediation strategies.

“The community helps each other, but that is trust based.”

Small-business exposure was identified as another area requiring particular focus, with their relative lack of skills meaning they face only one choice: pay or go out of business.



That ever-present risk means that companies should stop trying to take the easy way out by paying ransoms.”



Ultimately, the panel agreed, better transparency around ransomware attacks, payments, and remediation would help every Australian organisation to be better prepared for an attack – and ready to respond in a way that has already gained broad internal support from board members, legal, technical, and other staff.

“Transparency is the reason organisations can turn things around so quickly,” one delegate said, “and the industry comes together to accelerate the collective response when there is an incident.”

Discussions about ransomware must be “removed as a taboo topic,” the delegate said, “and the habit of avoiding media attention needs to go away.”

mimecast

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.