ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

JULY 12, 2021

EU Spotlight: Top 6 Issues All General Counsel Need to Know About Ransomware

by Kim Peretti, Kate Hanniford, and Riven Lysander

Ransomware has become an increasingly lucrative criminal industry that is projected to cause over €16 billion in global damages to companies in 2021. Some estimates are even higher, with one global security company calculating that the true global cost of ransomware, including business interruption and ransom payments, ranged from €35 billion to €142 billion in 2020. As one indication of the escalating threat landscape in the EU, the EU Agency for Cybersecurity (ENISA) reported 304 significant, malicious attacks against critical sectors in 2020, compared to 146 in 2019. These attacks can result in disrupted or even crippled operations, with network downtime costing companies an average of nearly €4,700 per minute—over €280,000 per hour—as evidenced by the fallout of the attack on the Irish Health Service Executive in May 2021, which remained significantly disrupted for weeks after the attack, and one of the largest Swedish grocery chains, which was forced to shut down 800 stores after an unprecedented ransomware supply chain attack against an IT management software provider. As companies continue to enhance their security and restoration capabilities to prevent or minimize the impact of a successful attack, ransomware actors likewise continue to escalate threats and adapt their tactics to overcome these measures.

1. Payment will not result in zero impact

Ransom demands are growing—the average ransom paid nearly tripled from approximately €97,000 in 2019 to €260,000 in 2020—but a payment does not guarantee zero impact. Attackers may attempt to leverage victims by claiming that it is more cost-effective to pay the ransom and keep quiet than to pay the costs associated with GDPR compliance and potential associated notifications. Indeed, GDPR compliance requirements may be triggered if personal or sensitive data is unable to be fully recovered or restored.

According to the Ponemon Institute, the cost of lost business is the largest cost factor in determining the total cost of a data breach. Irrespective of whether a ransom is paid or whether data is restored from backups or via a decryption tool, ransomware attacks typically involve significant downtime, and that downtime is increasing. A reputable third-party ransomware intermediary has reported that the average downtime following a ransomware attack increased from 19 days in the third quarter of 2020 to 21 days in the fourth quarter of 2020 *regardless of whether the company paid for a decryption key*. Is your company prepared to be down for over three weeks? For example, the Danish facility management services company ISS needed over a month to regain control of critical business applications. After a

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

DKK 365 million (€49 million) IT infrastructure rebuild, all systems were finally completely recovered just over a year after the incident.

In addition, paying a ransom generally does not guarantee that a company will be able to restore all of its data immediately, or at all. Several factors—including the ransomware variant, the threat actor group, and the configuration of the company's systems—can contribute to whether a company will be able to partially or fully decrypt its data if it is not in a position to restore its system and data without paying for a decryption key.

The likelihood of downtime and the inherent uncertainty surrounding restoration following a ransomware incident have resulted in an increasing need for robust incident response and resilience planning. In particular, companies may be especially well-served by incorporating a ransomware playbook into their existing incident response plans and ensuring their incident response teams have practiced multiple ransomware scenarios in tabletop exercises, for example.

2. Check your cyber-insurance coverage ... and be prepared for the renewal process

The increasing frequency of ransomware attacks and rising costs of ransom payments have placed renewed focus on the particulars of cyber-insurance coverage. Although some cyber-insurance companies provide broad coverage, including both incident response and forensic assistance to aid in timely operational recovery, global insurance company AXA recently took the first step in moving the industry away from cyber-insurance policies that reimburse insureds for ransomware payments by suspending the option in France. Even if a policy does cover ransom payment reimbursement, however, an insurer is likely to reevaluate the policy and premium after the incident.

Because the increasing costs of ransom payments have placed strains on the insurance industry, insureds can expect that the underwriting and renewal processes may be more rigorous than in previous years. Indeed, as companies seek to acquire new cyber-insurance policies or renew existing ones, the insurers' enhanced diligence procedures may require additional disclosures or the implementation of new or more stringent cybersecurity procedures to meet the insurer's standards. Policies can often require a checklist of specific security controls designed to mitigate the risk of ransomware to be in place and periodically tested for effectiveness, for example.

There is also the risk that an insured company may find that its policy's pre-approval process for the retention of outside counsel, forensic experts, ransom payment facilitators, and even the potential ransom payment itself is in tension with the company's interest in a swift and immediate response to the ransomware event. The extent to which the policy includes recovery costs can pose an additional challenge if a policy does not treat expenses related to the forensic investigation, the ransom payment itself (if applicable), and rebuilding affected systems as covered recovery costs.

3. Double extortion

As companies grapple with the challenges associated with improving security and recovery capabilities, organized criminal groups associated with ransomware attacks have undergone a period of reorganization and shifting of tactics that may frustrate response efforts. For example, in the second half of 2019, threat actors began using a wider range of techniques to incentivize the payment of ransom, chiefly by exfiltrating data before executing the ransomware and then threatening to post victims' identities and data through online "shaming" boards. This trend accelerated in 2020 and into 2021, beginning with Sodinokibi's use of a double extortion scheme to target Travelex, the world's largest chain of currency exchange shops in early 2020. More recently, the Conti group targeted the Irish Department of Health and the Health Executive Service in May 2021, threatening to sell or publish private data after crippling the health and social service systems for the entire nation of 4.9 million people. An interesting twist to this incident is that the Irish authorities made clear that they would not pay the $20 million ransom and the threat actors responded by providing the decryption tool for free, but then proceeded to leak some patient data when the ransom was still not paid. According to one security firm, the percentage of ransomware attacks that involved the threat to release stolen data on the dark web increased from 50% in Q3 of 2020 to *70% in Q4 2020*. Are you prepared to have your sensitive data leaked on a criminal site?

Not surprisingly, this second threat of data leakage may also lead to more complicated regulatory issues. Having personal or sensitive data leaked significantly increases the risk that the event will trigger GDPR notification requirements. Forensic and threat intelligence firms also report that threat actor groups have shifted the type of information targeted for encryption or exfiltration in attacks. Whereas individuals' personal information has long been targeted, recent incidents such as the attack on a Polish game developer highlight the extent to which sensitive corporate information and intellectual property are valuable targets.

4. Paying the ransom might not be an option

Both EU regulators and insurance companies have recognized the proliferation of ransom demands and staggering amounts of cyber-extortion payments when viewed in the aggregate, and this recognition marks a watershed in the approach to ransom payments as a result of recent regulatory guidance and increased expectations for compliance. For example, global insurer AXA's decision to remove the option to sign policies that reimburse victim companies for a ransom payment was apparently driven by French officials' concerns about the growing threat of ransomware.

Insurance coverage may not be the only concern, however. On July 30, 2020, the Council of the EU developed its first cyber-sanctions regime targeting a number of actors, including four Russian GRU members, two Chinese nationals, and North Korean firm Chosun Expo for the WannaCry, NotPetya, and Cloud Hopper attacks. These sanctions prohibit the direct and indirect release of funds to the sanctioned actors and applies to all Member States, and their governing framework has been extended through May 2022.

Other country-specific sanctions regimes may apply as well, such as a provision of the UK's Terrorism Act 2000, which prohibits an entity from providing money or property to an actor if the entity "knows or has reasonable cause to suspect that [the money or property] will or may be used for the purposes of terrorism." Accordingly, there are circumstances where even if a company was inclined to pay the ransom to mitigate the risk to impacted data, it may not be able to lawfully do so.

As European and other agencies increase their scrutiny of such payments, insurers and some third-party payment facilitators have similarly bolstered their compliance procedures to insulate themselves from further risk. For example, some third-party payment facilitators now maintain a more stringent "no-fly" list than the UK's Terrorism Act and U.S.'s OFAC Specially Designated Nationals and Blocked Persons List. Some insurance companies will now require more rigorous certifications of compliance with other extraterritorial and international provisions. Consequently, there are additional circumstances where even if a company may be able to lawfully pay the ransom, third-party payment facilitation or insurance reimbursement for the payment may be unavailable.

In sum, companies are well-served by preparing for circumstances where a company is precluded from payment—either as a matter of legal compliance, company policy, or other practical or contractual considerations. To further exacerbate the situation, because ransomware attacks are now frequently a two-step extortion process, where payment is demanded in exchange for a decryption key and then to prevent data leakage of any exfiltrated data, the consequences of nonpayment can be significant. In instances where ransomware payment is not an option and data has been exfiltrated before encryption, the need for secure backups and a comprehensive incident response plan as a starting point for recovery is especially important.

5. Expect increased obligations from the new EU Joint Cyber Unit and guidance from the UK Information Commissioner's Office

In response to the increasing number of cybersecurity incidents—including the dramatically increasing rate of ransomware attacks—the EU has proposed a new cybersecurity task force for a unified European response to cyber incidents, including ransomware. The "Joint Cyber Unit," led by ENISA, would allow Member States to seek help from other Member States. This assistance could include the deployment of a rapid response team to fight hackers during "real time" as an attack is unfolding.

Additionally, during the Information Commissioner's Office (ICO) May 2021 Data Protection Practitioners' Conference, the ICO announced that new guidance on ransomware is forthcoming. The new guidance will include advice on preparation; data protection requirements; and incident response plans, notification, and compliance. Currently, the ICO begins a ransomware investigation by looking at the affected entity's GDPR compliance posture—particularly focusing on Articles 5 and 32 initially—and whether the entity has segregated its live and offline repositories to ensure compartmentalization. The new guidance may contain provisions for increased obligations for victim companies.

6. Proliferation of guidance … it's back to the basics

Organizations have no shortage of guidance available to them from law enforcement and regulatory authorities regarding the ransomware threat and steps to mitigate it. Recent guidance ranges from the UK National Cyber Security Centre (NCSC) guidance on mitigating malware and ransomware attacks to mitigation strategies in ENISA's 2020 Ransomware Threat Landscape Guide to general guidance. There are growing collaborations between private and public sector actors, such as the joint Ransomware Task Force, composed of tech companies such as Amazon, Cisco, FireEye, Microsoft, and McAfee, and multinational agencies such as Europol, the UK National Crime Agency, and the U.S. Department of Justice, as well as NoMoreRansom.org, a joint effort by the Dutch National Police, Europol, McAfee, and Kaspersky Lab.

A common thread that runs through ransomware guidance—irrespective of an organization's market sector, size, or nature—is the importance of certain security controls that fall squarely within basic cyber-hygiene and well-established principles of reasonable security.

Initial guidance on earlier ransomware variants focused on the need for reliable backups; however, the additional threats posed by data leakage, targeted attacks, and increased guidance (and therefore increased expectations for resiliency) have prompted a corresponding focus on basic cybersecurity controls that can be especially helpful in preventing or minimizing the impact of ransomware incidents. Although maintaining proper backups continues to be a core measure to reduce the amount of downtime, additional measures include minimizing the potential success of phishing incidents, which can serve as a gateway incident to more serious ransomware attacks. The implementation of email security measures such as multifactor authentication and increased training, including simulated phishing emails, can ensure users are appropriately aware of the risks. Organizations should consider disabling remote desktop protocol (RDP) access because it permits attacks to circumvent endpoint detection tools and facilitates easier lateral movement within a network. In addition, patching vulnerabilities according to manufacturer's specifications and applying the latest updates may prevent vulnerability exploitation. Given the trend for zero-day vulnerabilities to be exploited, it may not be sufficient to rely on traditional patch management schedules.

In conclusion, the evolving threat tactics associated with ransomware attacks continue to pose practical challenges for companies. In situations where either the company's backup capabilities or ability to pay the ransom to prevent data leakage is suboptimal, ransomware events now easily reach "mega-breach" proportions in terms of their impact to the victim company. This is especially true when a company faces a costly recovery process that can include a ransom demand, technical restoration, a forensic investigation, dark web monitoring, and legal notifications—costs that may or may not be covered by a cyber-insurance policy. And while certain aspects of the ransomware threat landscape are beyond a company's control—in particular the ransomware variants and threat actor group tactics—factors such as insurance coverage, the sufficiency of existing security controls in light of current threats, sanctions compliance, incident response planning, and information-sharing arrangements can be addressed proactively by a company in the course of its incident response planning and preparation efforts.

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our **publications subscription form**.

Learn more about our **Privacy, Cyber & Data Strategy Team**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

ALSTON & BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2021

ATLANTA: One Atlantic Center ▪ 1201 West Peachtree Street ▪ Atlanta, Georgia, USA, 30309-3424 ▪ 404.881.7000 ▪ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ▪ Suite 21B2 ▪ No. 7 Guanghua Road ▪ Chaoyang District ▪ Beijing, 100004 CN ▪ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ▪ Place du Champ de Mars ▪ B-1050 Brussels, BE ▪ +32 2 550 3700 ▪ Fax: +32 2 550 3719
CHARLOTTE One South at The Plaza ▪ 101 South Tryon Street ▪ Suite 4000 ▪ Charlotte, North Carolina, USA, 28280-4000 ▪ 704.444.1000 ▪ Fax: 704.444.1111
DALLAS: Chase Tower ▪ 2200 Ross Avenue ▪ Suite 2300 ▪ Dallas, Texas, USA, 75201 ▪ 214.922.3400 ▪ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ▪ Building 3 ▪ Suite 150 ▪ Fort Worth, Texas, USA, 76107 ▪ 214.922.3400 ▪ Fax: 214.922.3899
LONDON: 5th Floor ▪ Octagon Point, St. Paul's ▪ 5 Cheapside ▪ London, EC2V 6AA, UK ▪ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ▪ 16th Floor ▪ Los Angeles, California, USA, 90071-3004 ▪ 213.576.1000 ▪ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ▪ 15th Floor ▪ New York, New York, USA, 10016-1387 ▪ 212.210.9400 ▪ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ▪ Suite 600 ▪ Raleigh, North Carolina, USA, 27601-3034 ▪ 919.862.2200 ▪ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ▪ Suite 2100 ▪ San Francisco, California, USA, 94105-0912 ▪ 415.243.1000 ▪ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ▪ Suite 430 ▪ East Palo Alto, California, USA 94303 ▪ 650.838.2000 ▪ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ▪ 950 F Street, NW ▪ Washington, DC, USA, 20004-1404 ▪ 202.239.3300 ▪ Fax: 202.239.3333