# The Evolution of Data Breach Threat Actors and Response

**By: Amy R. Worley and Marc Dautlich[1]**

A common approach to cyber security incidents used to be that upon discovery, companies would consult with their legal counsel and then engage with IT forensic experts before deciding whether to notify regulators and individuals that their systems or data had been compromised. More recently, threat actors have been following through early on their threats to publicise incidents, so weakening such attempts by companies to maintain control of the public narrative and increasing the pressure to pay the ransom demand. This is reducing the time available to companies for decision-making. It is also increasing the frequency with which the handling of such incidents is conducted from an early stage in the full glare of publicity, in circumstances where affected individuals, regulators, claimant law firms and other interested parties already know some of the details of such incidents.

Such tactics serve to underscore the value of investing time in advance planning for handling cyber incidents. Advance planning is perfectly possible, and it has the potential significantly to reduce damage to reputation and costs of handling.

First, a little more about the nature and scale of the threat.

## Ransomware as a Service

Evidence from a range of security surveys suggests that ransomware groups are the predominant current form of cybercrime carried out for financial reasons (as opposed to cyber incidents resulting from politically motivated attacks, activism and espionage).

Ransomware groups evolved considerably during the pandemic. Evidence from forensic investigations and intelligence from law enforcement has for some time suggested that ransomware groups organised themselves in ways that mimic the conventional economy. Thus, 'Crime as a Service', and 'Ransomware as a Service'[2] (RaaS) were offered online by organised groups to criminal SMEs and criminal entrepreneurs, sometimes in packages not much different to conventional software-and-services offerings. These offerings now apparently include 'starter' ransomware packages available online as little as twenty dollars, with premium 'add-on' services available for additional payment[3].

> *Entry-level criminal endeavours not working? Have you thought about upgrading to our premium services, where you'll find a range of enticing criminal bolt-ons? Take your criminal endeavours to the next level with our new 'Distributed denial of service software and support' feature! A steal this month at only $99! For real criminal peace-of-mind, add 24/7 support for as little as $29.99 a month!*

Further mimicking conventional business structures, ransomware groups are also increasingly specialised. Some groups have developed particular areas of expertise. For example, in

[1] Ms. Worley is a Managing Director and Associate General Counsel at Berkeley Research Group, a global consultancy firm. Mr. Dautlich is a Partner at Bristows LLP, a law firm headquartered in London, UK. Both Ms. Worley and Mr. Dautlich focus on IT, data protection, and data breach response. This paper was submitted in September 2022.

[2] *Enisa Threat Landscape for Ransomware Attacks*, July 2022, 4.2-4.3, p. 16

[3] Experian, In Conversation, September 2022

reconnaissance of potential industry verticals or even individual companies as targets. Or the aforesaid support services available for use by the less technically-adept players. Others still specialise in 'reputation management', ensuring that market participants maintain industry reputation by honouring the bargain to decrypt or repatriate stolen data once the ransom is paid.

This professionalization of ransomware attacks involves co-ordination, using the following forms of leverage to maximise the chances that a target organisation will pay:

i. trying to impact the productivity of the business by shutting off access to data required to execute key business processes;
ii. targeting elements of healthcare provision or safety-related supply chains to compromise safety;
iii. threatening to publicise incidents and tip off claimant law firms about potential classes of claimants impacted by a ransomware attack.

## Organisational Readiness

When asked about their readiness for cyber-attacks, Experian reported that 72% of business leaders said they are ready but in reality only 50% had a plan in place and 30% had never tested their plan. One organisation's plan was apparently in a two-year-old Word document where every individual in the incident team in the plan had left the organisation.

All too commonly, no effective planning had been undertaken about the practicalities of how a business would, in fact, contact affected individuals or manage any ongoing communications with those individuals. The question of how to communicate in the event that a firm's email system was temporarily unavailable was altogether too complex to plan for. Moreover, many companies who have relatively up-to-date incident response plans often have not tested them either in tabletop exercises or simulated "live" attack events so that flaws in the plan can be identified and remediated prior to facing a true exploit.

Looking at one particular area of incident response planning (notification to affected individuals), there are just four steps that will increase the effectiveness of such planning in the area of timely and effective notification to affected individuals; (some of these steps will also improve a firm's compliance with data protection and data privacy requirements more generally):

i. deduplication and 'cleaning' of email records, so that the organisation has the practical means to contact affected individuals, whether they be staff, former staff, customers, business partners or other stakeholders
ii. advance preparation of templates for each different group of affected individuals. Such templates could contain checklists prepared in advance identifying formal legal requirements for notifications in relevant jurisdictions. They could also consider in outline the typical types of steps that affected individuals are recommended to take to reduce the risk of identity theft or similar harms
iii. design of a release model to stagger outbound communications to affected individuals, so as to increase the prospects of successfully managing peaks in the flow of inbound communications. It is surprising how often proper communication with the firm's own employees is overlooked in the early stages of an incident
iv. consideration of the channels by which affected individuals are to communicate with the organisation for further information (FAQs only? Live chat? Dedicated email? Other?)

## Legality and Ethics of Ransomware Payments

Various national regulators, such as the U.S. Office of Foreign Assets Control (OFAC) have issued strict guidance forbidding the payment of ransom to threat actors on the known sanctions list. Ransom negotiators must carefully vet payment to bad actors against the OFAC prohibited payments list, and similar other national regulatory lists. That said, so-called "burner wallets" for payments of cryptocurrency, and the ability to obscure IP addresses and other identifiers via anonymizing tools such as Tor, makes some of these prohibited payment rules relatively easy for threat actors to avoid. Governments across the world are still trying to align on the best method for addressing this somewhat anonymous and shifting threat.

Even where there is no explicit law or regulation prohibiting ransom payments there are ethical and policy considerations to such payments. As long as companies continue to pay ransom, ransomware threats will persist, if not increase in frequency. As discussed above, many cyber criminal organizations consider themselves legitimate businesses with departments tasked with making the ransom negotiation experience as "pleasant as possible" so that victim companies will share their experience in getting functioning decryption keys, albeit at a very steep price, thereby increasing the chances that other victims will choose to pay ransom.

There are multiple considerations in determining whether it makes good legal, business, and ethical sense to pay a ransom demand, including:

i. whether there is a national law or regulation making such payments unlawful
ii. whether ransom payment is consistent with company values
iii. whether the threat actor exfiltrated data that they may use later to come back again and ask for additional payments
iv. whether the company has sufficient back-ups to remediate the situation without the need to decrypt the information

## Attorney Client Privilege During the Attack investigation.

Companies must also be wary of over-relying on attorney-client privilege and secrecy standards in responding to data breaches. Laws vary, of course, by jurisdiction, but increasingly courts and regulators are requiring data breach and ransomware victims to produce forensic investigation evidence, even where it was conducted at the request of outside counsel. Two cases in the U.S. recently, held that the forensic investigation into the breach was not "legal advice" but was a business response to the attack. Accordingly, those reports had to be produced in litigation. In order to preserve some level of confidentiality in working with attorneys in response to breaches, companies must consider:

i. bifurcating the investigation into portions directed by counsel and for the purpose of obtaining legal advice and the technical analysis of how to prevent future attacks
ii. the national rules, court decisions, and regulatory impact of limitations on attorney-client privilege
iii. the nature, breadth, and content of what is documented about the breach investigation and response

## Resources

The threat landscape and legal obligations are constantly evolving. Attached to this paper are legal resources that in-house counsel and outside counsel should consider when responding to breaches. They are by no means comprehensive globally but do provide timely examples of the legal, financial, and on-going security considerations companies face in responding to data breaches. These resources include:

- **The European Data Protection Board (EDPB) Guidance on Data Breach Response**
- **U.S. Federal Trade Commission Guidance on Data Breach Response**
- **The OFAC guidance on ransomware payments**
- **Recent caselaw out of the U.S. limiting the application of the attorney client privilege in data breach response cases.**
- **Cybersecurity Basics for Small Business**
- The IBM/ Ponemon Report on the Cost of Data Breaches in 2021