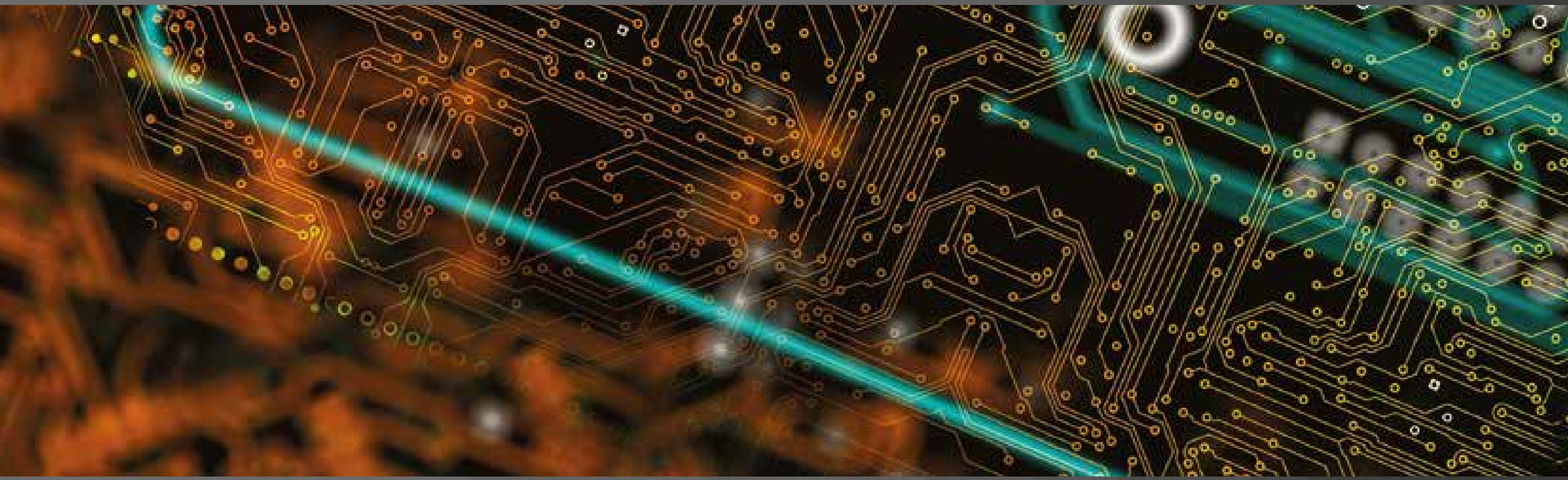
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

Q&A Chapters

Get Stuffed! Are You Prepared for a Credential-Stuffing Attack?

Nigel Parker

Nathan Charnock

Allen & Overy LLP

Introduction

Cybercrime is estimated to cost the global economy $600 billion per year,[i] with over 15.1 billion records exposed by data breaches across the world during 2019.[ii] In recent years, and particularly during the onset of the COVID-19 pandemic in 2020, there has been a significant growth in the use of "credential stuffing" as a mode of attack.

These incidents involve an automated system, or "bot", exploiting genuine login credentials, likely stolen from another compromised website, or gained via phishing or other techniques, to try to gain access to a user account on a (previously uncompromised) website. Highlighting how easy it is to obtain compromised credentials, in early 2019 hackers posted an aggregated credential collection that contained the results of multiple data breaches, totalling 2.2 billion unique username and password combinations, all available to download for free. Shortly after, a further 841 million records were made available on the dark web, from 32 websites and apps, including MyHeritage and MyFitnessPal.

Whilst the primary motivation for these attacks is financial – gaining access to your online banking account or to a retail website where your payment card details are stored – access to user accounts can furnish the perpetrators with huge volumes of personal data for use in identity theft.

Many people use the same username and password combinations across multiple websites and credential-stuffing attacks take advantage of this behaviour. The dark web provides a lucrative underground marketplace within which billions of stolen account credentials can be bought and sold. Using a "bot" allows a criminal to scale up the process, enabling thousands of login attempts to be made in parallel, using different stolen credentials across multiple websites.

Companies who fall victim to these attacks can really pay the price; whilst reputational damage, regulatory fines and litigation costs can be significant, a credential-stuffing attack can also overwhelm your website and other technical infrastructure, causing severe business impact and putting a strain on IT, customer services and other resources.

So how do you prepare for a credential-stuffing attack? And how do you react when one occurs?

Preparing for a Credential-Stuffing Attack

Know your enemy

As is the case with other types of cyber-attack, companies should ensure they have, within their ranks, individuals with sufficient understanding of how credential-stuffing attacks typically materialise.

Credential stuffing is reasonably unsophisticated and easy to scale; the "bots" used are often off-the-shelf and readily available online, some free of charge! This makes it a popular weapon for cybercriminals. One of the most successful ways of "stuffing" is the "low and slow" method, which sees attackers hide their attack amongst a smokescreen of legitimate traffic, whilst limiting the number of attempts made. However, the more attempts made, the more valid login credentials will be identified. Just one data breach can put many other businesses at risk, as it can allow further unauthorised logins without breaching a company's infrastructure or triggering any security alerts or measures.

Companies should ensure they keep up to date with events and trends in this space and use that knowledge to inform their cybersecurity planning. Regular scanning of published lists of compromised credentials can also help head-off attacks.

Proactive monitoring

Proactive monitoring is one of the most effective tools to enable cybersecurity teams to identify and respond quickly and efficiently to credential-stuffing attacks. The National Cyber Security Centre recommends that businesses model their user login patterns and set-up of alerts, notifying the relevant IT monitoring teams of unusual activity or high volumes of traffic. For example, alerts could be set up to identify an increase in failed login attempts across numerous accounts, higher than normal volumes of foreign IP addresses or anomalies in browser activity that may indicate the use of automation. Companies can also use analytics to assess if a login attempt is authentic; for example, this could include ensuring the location and IP address of any login attempt is checked against the last successful login attempt, to allow a credibility judgment to be made in respect of each request. There are a number of third-party providers and tools on the market to assist businesses with monitoring activity.

Improve underlying security measures

Whilst monitoring can help companies to identify and respond to incidents, businesses should primarily focus on prevention techniques. Three things are needed to perpetrate credential stuffing: (i) a list of credentials; (ii) a target (this could be a general login on a web page or an API endpoint); and (iii) a bot or mechanism to leverage the stolen credentials. A number of tools can be leveraged to prevent access to the first and the second. Sadly, the bots are still widely available online.

1. **Protect the credentials**

   There are a number of things individual users can do to ensure that, even if their credentials are stolen, they can protect themselves and the businesses they work for or have a relationship with. However, for businesses, the best way to protect against credential stuffing is to:

- encourage individuals to set unique passwords for different websites that they use;
- implement rules requiring passwords to contain a minimum of eight alphanumeric characters and a mixture of characters, including symbols; and
- force passwords to be reset periodically.

2. **Protect the target website login page or API**
   Between May and October 2019, 75% of login attacks against financial services companies involved credential stuffing targeting APIs.[iii] When designing its API or website login page, a business should ensure it takes a number of steps to mitigate the risk of a successful credential-stuffing attack such as:
   - implementing multi-factor authentication;
   - enabling human verification systems such as reCAPTCHA;
   - using geofences to block proxy traffic that comes from certain jurisdictions, enabling access only from those jurisdictions where the business operates or provides services;
   - limiting the number of failed login attempts that can occur before locking the account and alerting the individual account owner of an issue;
   - using device or browser fingerprinting and requesting more information from users if they login from unknown devices;
   - using a neutral message for failed login attempts – for example if a "bot" enters a correct username but an incorrect password, do not inform it that "your password is incorrect" as the "bot" will know the username is correct;
   - run a TOR node to carry out additional checks on authentication attempts; and
   - deploy a network-based bot management solution as part of a multi-layered security implementation – these tools detect and control illegitimate bot traffic at the network edge, blocking attackers before they can get to your applications or overwhelm your infrastructure. Leading bot management platforms use artificial intelligence and machine learning to detect and thwart advanced credential-stuffing attacks.

It is worth noting that, as set out in this *International Comparative Legal Guide*, there are a number of legal obligations relating to cybersecurity that must be met by businesses. For example, under the GDPR, firms are required to process personal data securely by means of appropriate technical and organisational measures and they must take into account "the state of the art" when deciding what is appropriate. The state of the art continues to evolve and businesses should ensure their protections against credential-stuffing attacks evolve with this.

Incident response plan and procedures

Companies should ensure they have detailed incident response procedures in place and should conduct regular testing of these procedures to ensure relevant personnel understand their roles.

Access to appropriate expertise

It is strongly recommended that, as part of cybersecurity response planning, businesses ensure they have appropriate relationships and arrangements in place with a number of third-party advisors who can be called on, at short notice, to assist in the event of an incident, such as specialist cyber advisors and forensic IT experts, legal advisors and PR consultants.

Consider proactive measures

Google recently launched its "Password Check-up" feature which is built into its password manager, and therefore its Google Account and Chrome products. Password Check-up assesses the strength and security of all your saved passwords, tells you where Google finds they have been compromised in prior breaches and gives you personalised actionable recommendations when needed.[iv] This provides proactive protection for individuals, and if done without diminishing consumer experience or blocking legitimate traffic, it could be an effective tool to mitigate the risk of credential stuffing.

What Does an Effective Response to a Credential-Stuffing Attack Involve?

Implementing the measures outlined above will mitigate the risk of your business and your users from falling victim to a credential-stuffing attack. However, if an attack does occur, how should you respond? Each incident will present a unique set of circumstances, but we have set out below some of the steps you may need to take.

1. **Establish the facts** as quickly as possible to enable you to understand the scale and impact of the attack, including, amongst other things, when and how the attack took place, what information is known about the attacker (for example, is the same IP address being used?), the success rate of login attempts, the number of accounts accessed, the types of personal information accessed by the attackers, the value and nature of any financial loss to users or the business and whether other systems or group websites were affected/accessed.
2. **Instigate incident management procedures** involving key stakeholders from across the business which may include representatives from IT, security, legal, customer services, communications/public relations and the relevant product/corporate representatives and ensuring detailed incident logs are maintained to record decisions.
3. **Take initial remediation steps** in an attempt to stop the attack and prevent recurrence. This may involve, amongst other things: (i) temporarily suspending access to the API or login page, either in its entirety or from certain jurisdictions or IP addresses; (ii) conducting searches of the dark web to see if it is possible to identify if credentials have been stolen directly from your business for use in the attacks; (iii) deploying bot management solutions or adapting the way they are used; (iv) force-resetting user passwords to randomly generated passwords and requiring them to set a new password when they next log in; and (v) hiding payment card details or suspending cash-out or withdrawal options available on a user's account.
4. **Inform senior stakeholders** of events to ensure they are up to speed and able to take important decisions quickly, including dealing with any media interest.
5. **Instruct third party advisors** such as external IT/cyber consultants to help investigate and stop the attack and prevent reoccurrence, external legal counsel to advise the legal implications of the incident and to assist with regulatory reporting and PR/media consultants to help manage external and internal communications relating to the incident.

6. **Consider notifying law enforcement** – depending upon the nature, scale and severity of the credential-stuffing attack and local legal requirements, you should consider notifying law enforcement about the incident, as they may be able to assist with the investigation.
7. **Consider regulatory reporting obligations** that often require notifications to be made to the relevant regulator within a short time period (in some cases within just a few hours) after detection. In many jurisdictions, there are specific reporting requirements that apply to certain sectors, such as financial services and telecommunications whilst listed companies may have certain disclosure obligations that need to be met. Credential-stuffing attacks inherently involve the use of and access to personal data, so will often result in personal data breaches that in many jurisdictions may trigger an obligation to report to a data protection supervisory authority.
8. **Consider individual notification obligations** – there may be obligations under local legal requirements to notify affected individuals about the attack. For example, in the EU and the UK, the GDPR requires individuals to be notified without undue delay of personal data breaches that could result in a high risk to their rights and freedoms. There may also be circumstances in which you would choose to voluntarily notify individuals about the incident so that they can take certain steps. In any event, it will be important to ensure that:
   a. individuals are provided with all information required by law;
   b. practical and sensible advice is provided such as advising individuals to:
      i. monitor their payment cards and bank accounts for suspicious activity and report any such activity to their financial service providers;
      ii. reset their passwords, using unique passwords for each of their online accounts;
      iii. consider using a password manager;
      iv. input their usernames and email addresses into https://haveibeenpwned.com/, to see if their credentials have ever been stolen; and
      v. consider using anti-fraud credit monitoring services (which you may offer to pay for);
   c. customer services teams have sufficient information and resources to respond to queries which may be received from customers following distribution of the notifications, including queries received via social media;
   d. the notice is reviewed by communications specialists and legal counsel to ensure it strikes the right tone; and
   e. clearly identify which individuals have been affected and should receive the notification to avoid over-notification if possible.
9. **Consider other notification obligations** such as contractual obligations to notify third parties of certain cyber-incidents or data breaches.
10. **Work with other interested third parties, such as financial service providers** – if customers have had money withdrawn or removed from their accounts or their financial account or payment card details have been stolen, you should consider liaising with financial service providers to help prevent further fraudulent activity using customer information.
11. **Complete a detailed incident review** to understand how the credential-stuffing attack was able to succeed, to analyse how the business responded to the incident and what lessons could be learned, and to identify and agree short-, medium- and long-term remediation actions to be taken across the business to prevent the reoccurrence of credential-stuffing attacks in the future.

The COVID-19 Effect

In early 2020, as the COVID-19 pandemic hit the world, millions of people globally were instructed to self-isolate and people turned to the internet more than usual, often working from home, and away from some of the security protocols that protected them in the office. An opportunity arose for cyber criminals, as security was traded for ease of access, with the use of outdated software, the mixing of personal and corporate emails, and the recycling of passwords between business and personal environments.

There was a large spike in malicious login attempts against European video service providers and broadcasters during the first quarter of 2020. One attack in late March 2020, after many isolation protocols, directed nearly 350 million attempts against a single service provider over a 24-hour period. Separately, one broadcaster was hit with a barrage of attacks over the course of the quarter, resulting in billions of login attempts. Cyber criminals began to retry their credential stuffing lists, like those mentioned earlier in this piece, and test them against services rising in popularity in the pandemic, such as Zoom, that saw usage rise from 10 million users to over 200 million users in the first few months.

Conclusion

Credential stuffing is increasingly the weapon of choice for cyber criminals seeking financial gain. For businesses, it has never been more important to evaluate your cybersecurity offering to ensure you are prepared the threat of these incidents. Whilst the criminals may sometimes remain a few steps ahead, the businesses who implement a range of security measures, use appropriate monitoring and reporting tools and deploy effective incident response procedures are well placed to tell the criminals to "Get Stuffed!"

Endnotes

i. McAfee, "Economic Impact of Cybercrime – No Slowing Down", Report, February 2018, p. 4.

ii. Risk Based Security, "2019 Year End Report, Data Breach Quickview".

iii. Akamai, "Financial Services – Hostile Takeover Attempts", Vol. 6, Issue 1, p. 2.

iv. Tuerk, A., "To stay secure online, Password Check-up has your back", Google Blog, 2 October 2019.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking proactive steps in response to attacks.

Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Nathan Charnock is an associate specialising in commercial contracts, data protection and privacy, intellectual property and information technology law. He advises clients on their response to cybersecurity attacks, including their interactions with regulators and implementation of remediation steps. Nathan also advises on complex commercial arrangements for a range of clients in the technology, retail, telecommunication, life sciences and financial services sector, including IP licensing, outsourcing and service provision arrangements.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3899
Email: nathan.charnock@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning over 40 offices. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.

We have a strong cybersecurity practice comprising a core team of 19 partners with diverse backgrounds in data protection, bank regulation, antitrust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Data Protection
Derivatives
Designs
Digital Business

Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law

Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by: glg global legal group