Threat research snapshot for Nestlé 2024

verizon business

Foreword

Verizon has compiled this overview of the cyber threat landscape for Nestlé. In it, we focus on insights most relevant to Nestlé and your specific security concerns. We share:

- The relevant findings from analysing 30,458 real-world security incidents, of which 10,626 were confirmed data breaches, with victims spanning 94 countries.
- Insight from our security experts, whose competencies include key regulations, frameworks, and threat intelligence.
- Additional knowledge we have gained from thousands of post-breach forensic investigations.

The recommendations provided within this snapshot do not necessarily constitute a proposal or an offer of service. They are provided to Nestlé solely as insight based on our extensive cyber thought leadership and the expert knowledge of our dedicated team.

We would be keen to learn more about Nestlé's security concerns and how our portfolio of solutions, vast expertise, and extensive ecosystem could help address them.

About Verizon's security practice

Verizon has been protecting enterprise IT infrastructure for over 20 years. This began with the acquisition of internet services provider (ISP) UUNET, followed by acquisitions of pure-play companies including NetSec, CyberTrust, Vidder, Niddel and ProtectWise.

We offer a wide range of services that span the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover). We particularly excel at managed security services, security consulting, SOC transformation and operations, and cyber incident response.

We also have significant partnerships with many top security vendors and have been rated a Leader in many security landscape reports by major analysts.

About the Data Breach Investigations Report (DBIR)

Every year, we consolidate, organise and analyse threat data from around 60+ partner organisations. The organisation of the data is carried out using the Vocabulary for Event Recording and Incident Sharing (VERIS) framework, an open-source framework for describing security incidents in a structured and repeatable manner, developed by Verizon. This analysis forms the basis of our annual Data Breach Investigations Report (DBIR). The first DBIR was published 16 years ago, the most recent in May 2024.

The report purpose

The DBIR provides security professionals with an in-depth analysis of data-driven, real-world instances of cybercrime and how cyberattacks play out. The past year has been a busy one for cybercrime. We analysed 30,458 real-world security incidents, of which 10,626 were confirmed data breaches (a record high in breaches!), with victims spanning 94 countries.

The Nestlé snapshot

As the world's largest food and beverage company, we understand your strategy[1] is to drive accelerated digitalisation by creating a seamless, data-driven consumer experience by prioritising e-commerce, leveraging AI, and remote assistance to enhance agility and flexibility in manufacturing and supply chains. As such, robust cybersecurity is crucial to protect your sensitive data and ensure operational resilience.

We understand from our briefing webinar that the DBIR insights help you focus on possible overlooked areas in security practices. The DBIR is a substantial publication—this year's report runs to 100 pages. To help you navigate the report and protect Nestlé, we've created this personalised snapshot focused on the concerns that you shared and the threats most relevant to you. Based on your feedback, we have focused this snapshot on enhancing cybersecurity measures against:

01	02	03	04
System Intrusion	Ransomware	Social Engineering	Supply Chain

As in previous years, we have also shared the highlights for the manufacturing sector.

We hope you can use this snapshot to increase your understanding of the threats and help you prepare Nestlé to handle them in the most effective and efficient manner possible.

2024 Data Breach Investigations Report

Get data-driven analysis of cybercrime in Verizon's annual DBIR.

Ransomware attack disrupts Dole's manufacturing operations

Dole, one of the largest fresh produce manufacturers globally, experienced a significant ransomware attack that led to the temporary shutdown of several production facilities in North America. The attack, caused by cybercriminals infiltrating Dole's systems and demanding a ransom, disrupted the supply chain, resulting in delays in shipments to grocery stores and affecting the availability of Dole salad kits in some regions. This incident highlighted the increasing vulnerability of the manufacturing sector to cyber threats, where operational disruptions had immediate and widespread impacts. Dole investigated the breach, involved law enforcement, and emphasised the critical need for robust cybersecurity measures in the manufacturing industry.

Source: https://therecord.media/dole-ransomware-attack-north-america

[1] https://www.nestle.com/about/strategy

DBIR extract: Food manufacturing

The food manufacturing sector is an attractive target for cybercriminals due to a reliance on interconnected systems and legacy technologies, which can have insufficient cybersecurity measures. These breaches not only cause financial losses but can also have far-reaching consequences on supply chains, affecting production and delivery of essential goods globally. In this year's report, manufacturing has seen an increase in Error-related breaches. The installation of malware after hacking via the Use of stolen credentials is also commonplace.

Industry classification explained

Industry classification enables us to identify patterns and analyse the types of incidents and attacks that industry sectors are susceptible to. The DBIR classifies incidents and breaches by industry vertical using the North American Industry Classification System (NAICS). The DBIR does not break out consumer packaged goods (CPG) companies but most of Nestlé's major business units fall within the manufacturing NAICS codes of 31–33. The Verizon Threat Research Advisory Center (VTRAC) found that the data for these groups showed very similar patterns to that of the overall manufacturing sector. So, for the purposes of this snapshot, we've looked at the larger datasheet to allow greater analysis.

2024 Manufacturing insights

This year's Manufacturing model comes with a new and improved feature: Errors! As in most other industries, Misdelivery is the error du jour, accounting for almost half (48%) of error-related breaches. This is in part the result of contributor bias, but nevertheless, sending things to the incorrect recipient does appear to be somewhat widespread regardless of vertical. Loss and Misconfiguration round out the top three error varieties, and they account for approximately 20% and 18% of breaches, respectively. System Intrusion continues to hold on to the top spot in Manufacturing. This is probably related to the still very effective combination of hacking via Use of stolen credentials (present in 25% of manufacturing breaches) to gain access to the environment and then the liberal application of Ransomware (involved in 35% of breaches in this vertical). It's hard to keep the gadgets rolling off the assembly line when your data is locked up tight and someone else holds the keys.

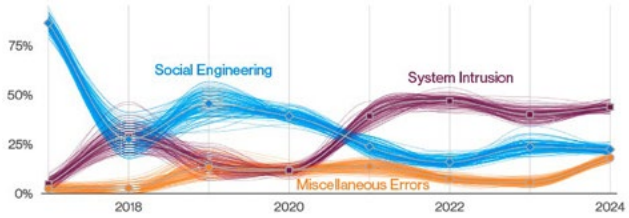


Figure 1. Top patterns over time in Manufacturing industry breaches

It's your asset on the (manufacturing) line

Social Engineering remains steady with regard to breaches in this vertical due to action varieties such as Phishing (55%) and Pretexting (42%). The Basic Web Application Attacks now languish near the bottom of the pattern rankings with the likes of Privilege Misuse. In fact, the asset of Server – Web app has been on a slightly downward trajectory. Figure 2 (below) illustrates this decline and shows the corresponding rise of Server – Mail. This makes sense when Phishing remains prevalent in the Manufacturing vertical. Of course, the credentials typically obtained via phishing are those that afford the criminal a foothold into the organisation via the email account of the victim.

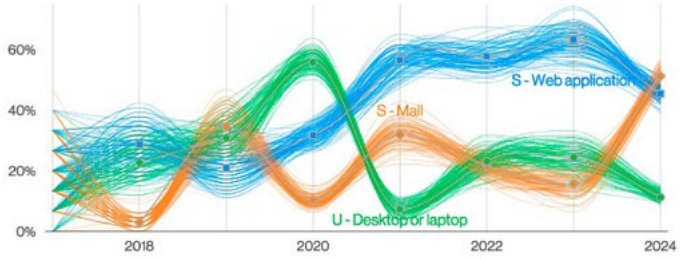


Figure 2. Top Asset varieties over time in Manufacturing industry breaches

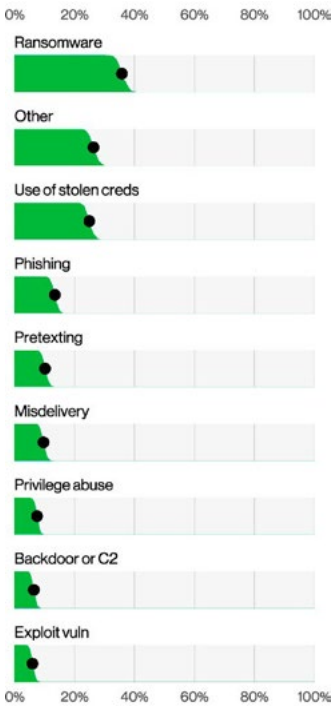
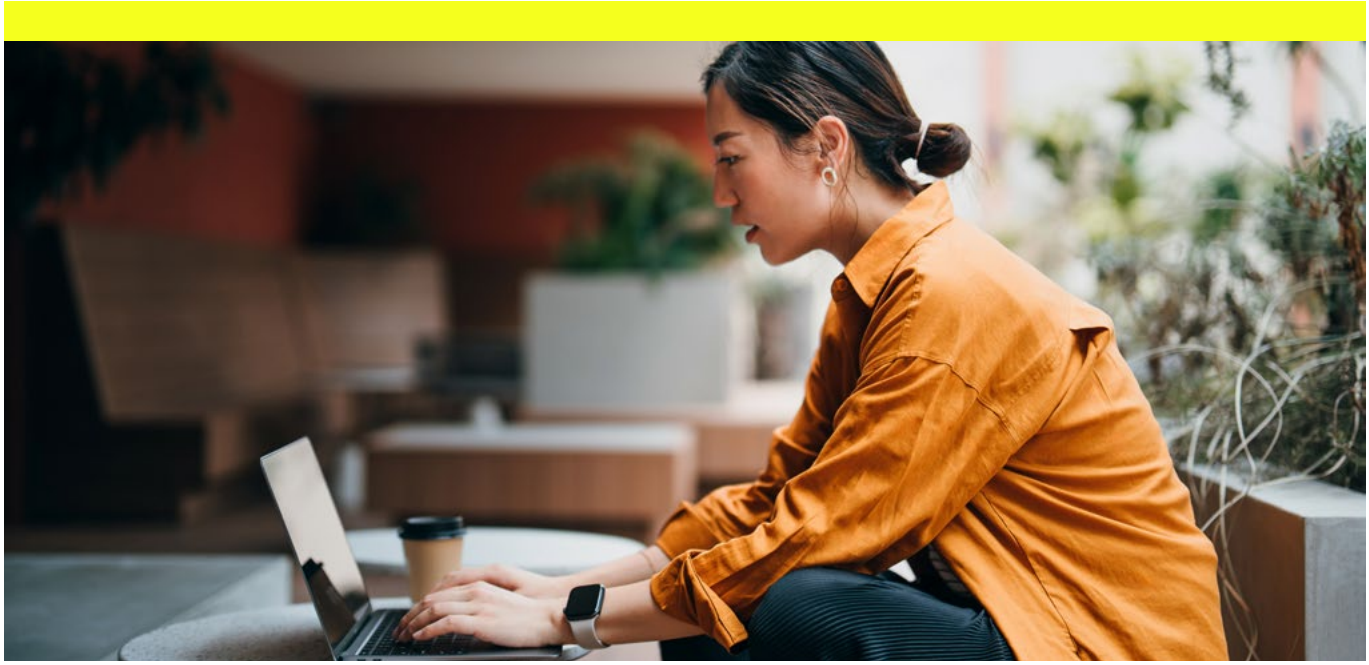


Figure 3. Top Action varieties in Manufacturing industry breaches



Facts snapshot

Frequency

- 2,305 incidents, 849 with confirmed data disclosure

Top patterns

- System Intrusion, Social Engineering and Miscellaneous Errors represent 83% of breaches

Threat actors

- External (73%)
- Internal (27%) (breaches)

Actor motives

- Financial (97%)
- Espionage (3%) (breaches)

Data compromised

- Personal (58%)
- Other (40%)
- Credentials (28%)
- Internal (25%) (breaches)

What is the same?

Two of the top patterns from last year are still in place. Financial motivation continues to be the driver behind most attacks.

DBIR Incident Classification Patterns

Basic Web Application Attacks:
Attacks against web applications.

Denial of Service:
Attacks on the availability of networks and systems.

Lost and Stolen Assets:
When an asset went missing, whether through mistake or malice.

Miscellaneous Errors:
Where unintentional actions directly compromised an information asset. This does not include lost devices, which are grouped with theft.

Privilege Misuse:
The unapproved and/or malicious use of legitimate privileges.

Social Engineering:
The compromise of a person that alters their behaviour into taking an action or breaching confidentiality.

System Intrusion:
Complex attacks that leverage malware and/or hacking.

Everything Else:
Any incidents that don't fit within one of the other patterns.

Four key risk areas for Nestlé to consider

01. System Intrusion

Summary

While shifts in tactics leveraged by Actors have modified some of the top Actions, the overall effect of these Actors continues to be felt by many industries and organisations of all sizes.

What is the same?

Ransomware attacks continue to drive the growth of this pattern as they now account for 23% of all breaches.

In the world of our attack patterns, it's been a competitive year, and there have been a lot of contenders vying for the first-place prize of MFB: most frequent breach. System Intrusion, for the third year in a row, leads the pack with 36% of breaches. The makeup of this pattern hasn't changed much. It is where our more sophisticated attacks are found. They still largely consist of breaches and incidents in which the threat actor leverages a combination of Hacking techniques and Malware to penetrate the victim organisation.

These Ransomware attacks account for 70% of the incidents within System Intrusion, as seen in Figure 4. The other often seen actions in the System Intrusion patterns tend to be those that provide the actor access to the environment, such as Exploit vulnerabilities and Backdoors. We also saw Extortion creeping into this space, primarily due to a large and impactful event.

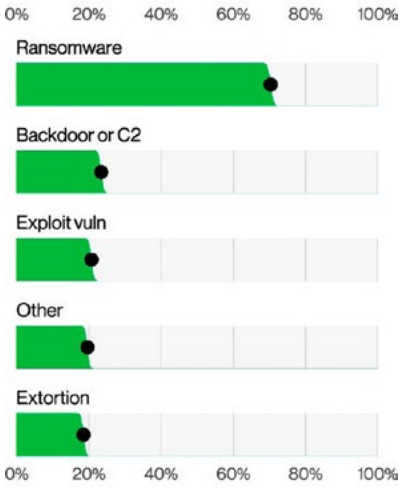


Figure 4. Top Action varieties in System Intrusion incidents

Relevant ATT&CK techniques

Exploit vuln (VERIS)

Exploit Public-Facing Application: T1190

Exploitation for Credential Access: T1212

Exploitation for Defense Evasion: T1211

Exploitation for Privilege Escalation: T1068

Exploitation of Remote Services: T1210

External Remote Services: T1133

Vulnerability Scanning: T1595.002

Use of stolen creds (VERIS)

Compromise Accounts: T1586

- Social Media Accounts: T1586.001
- Email Accounts: T1586.002

External Remote Services: T1133

Remote Services: T1021

- Remote Desktop Protocol: T1021.001

Use Alternate Authentication Material: T1550

- Web Session Cookie: T1550.004

Valid Accounts: T1078

- Default Accounts: T1078.001
- Domain Accounts: T1078.002
- Local Accounts: T1078.003
- Cloud Accounts: T1078.004

Execution: TA0002

Persistence: TA0003

Privilege Escalation: TA0004

Defense Evasion: TA0005

Credential Access TA0006

02. Ransomware

Ransomhow?

About vectors (Figure 5), we saw a great deal of Direct install. This is when threat actors use their existing system access to install malware, such as Ransomware or Backdoors. The vector of Web applications, which is a favoured target of exploits, also appeared frequently. We still see threat actors leveraging Email to reach users and Desktop sharing software to enter systems. Because these threat actors use a plethora of tools and techniques, this data is longer tailed, which is why other shows up relatively often in our top five. Within the category of Other are vectors such as VPNs, Software updates and a whole bunch of Unknowns (our bet is that it is most likely split among the tactics discussed above, just not explicitly reported to us). Therefore, when prioritising your efforts at protecting yourself, don't neglect addressing malware infections, stolen credentials or unpatched systems as it may lead you to break out in Ransomware.

Ransomwho?

Ransomware has again dominated the charts, accounting for 11% of all incidents, making it the second most common incident type. Ransomware (or some type of Extortion) appears in 92% of industries as one of the top threats. When we remove the Ransomware groups from this dataset, we're left with an even split of 44% run-of-the-mill types of criminals and 40% State-affiliated actors. It shouldn't be too surprising to find out that the tactics used by criminals are very closely aligned to those used by Actors working on behalf of their country. The major difference is what they do with that access. The subset of criminals in this pattern who aren't doing Ransomware/Extortion are quietly siphoning off Payment data from e-commerce sites and account for 57% of breaches involving stolen Payment cards, while the State-affiliated actors look to pivot and steal other types of data.

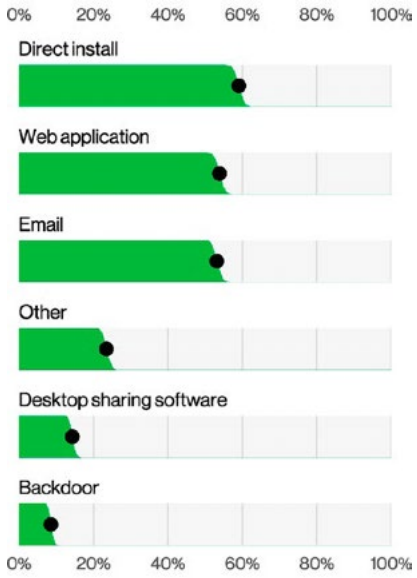


Figure 5. Top Action vectors in System Intrusion incidents (n=1,789)

Ransomwhat?

Understanding the cost associated with Ransomware is a bit complex as there are several primary and secondary costs to consider, not to mention the possible soft costs associated with reputational impacts. While we try our best to capture these costs, it's worth noting that the result isn't a full picture but simply our best approximation using the data we have. One of the easier costs to capture is the amount associated with paying the actual ransom. Analysing the FBI IC3 dataset this year, we found that the median adjusted loss (after law enforcement worked to try to recover funds) for those who did pay was around $46,000 as shown in Figure 6.

Figure 6. 95% and 80% confidence intervals of adjusted incident cost for Ransomware

This is a significant increase from the previous year's median of $26,000,

but you should also take into consideration that only 4% of the complaints had any actual loss this time, as opposed to 7% last year. Another way we can slice the data is by looking at ransom demands as a percentage of the total revenue. The median amount of the initial ransom demand was 1.34% of the victim organisation's total revenue—with 50% of the demands being between 0.13% and 8.30% (Figure 7). We know this is quite a spread for the initial ransom demand percentage. There were a few within the top 10% of cases reaching up to 24% of total revenue. Hopefully, these ranges assist organisations in running risk scenarios with an eye toward potential direct costs associated with a ransomware attack. Of course, many other factors should also be considered, but this is a good starting point.

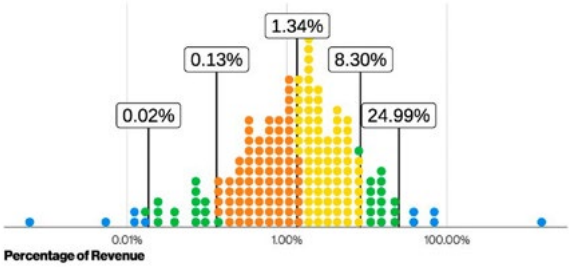


Figure 7. 95% and 80% confidence intervals of ransoms as a percentage of victim revenue

CIS Critical Security Controls for consideration

Bearing in mind the breadth of activity found within this pattern and how actors leverage a wide collection of techniques and tactics, there are a lot of safeguards that organisations should consider implementing. Below is a small subset of all the things Nestlé could do. Note the corresponding sections listed which can be found in the full report. They should serve as a starting point for building out your own risk assessments to help determine what controls are appropriate to your organisation's risk profile.

Protecting devices

Secure Configuration of Enterprise

Assets and Software [4]

- Establish and Maintain a Secure Configuration Process [4.1]
- Establish and Maintain a Secure Configuration Process for Network Infrastructure [4.2]
- Implement and Manage a Firewall on Servers [4.4]
- Implement and Manage a Firewall on End-User Devices [4.5]

Email and Web Browser Protections [9]

- Use DNS Filtering Services [9.2]

Malware Defences [10]

- Deploy and Maintain Anti-Malware Software [10.1]
- Configure Automatic Anti-Malware Signature Updates [10.2]

Continuous Vulnerability Management [7]

- Establish and Maintain Vulnerability Management Process [7.1]
- Establish and Maintain a Remediation Process [7.2]

Data Recovery [11]

- Establish and Maintain a Data Recovery Process [11.1]
- Perform Automated Backups [11.2]
- Protect Recovery Data [11.3]
- Establish and Maintain an Isolated Instance of Recovery Data [11.4]

Protecting accounts

Account Management [5]

- Establish and Maintain an Inventory of Accounts [5.1]
- Disable Dormant Accounts [5.3]

Access Control Management [6]

- Establish an Access Granting/Revoking Process [6.1, 6.2]
- Require MFA for Externally-Exposed Applications [6.3]
- Require MFA for Remote Network Access [6.4]

Security awareness programmes

- Security Awareness and Skills Training [14]

03. Social Engineering

Summary

Pretexting continues to be the leading cause of cybersecurity incidents, with actors targeting users with existing email chains and context. Extortion also grew dramatically because of the large-scale MOVEit incident.

What is the same?

Phishing and Pretexting via email continue to be the leading cause of incidents in this sector, accounting for 73% of breaches.

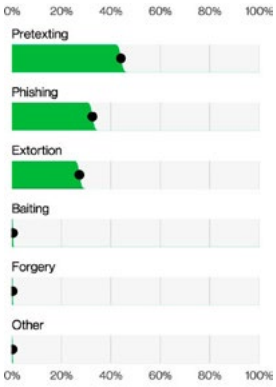


Figure 8. Top Action varieties in Social Engineering incidents (n=3,647)

Figure 9. Top Action vectors in Social Engineering breaches (n=2,961)

Facts snapshot

Frequency

- 3,661 incidents, 3,032 with confirmed data disclosure

Threat actors

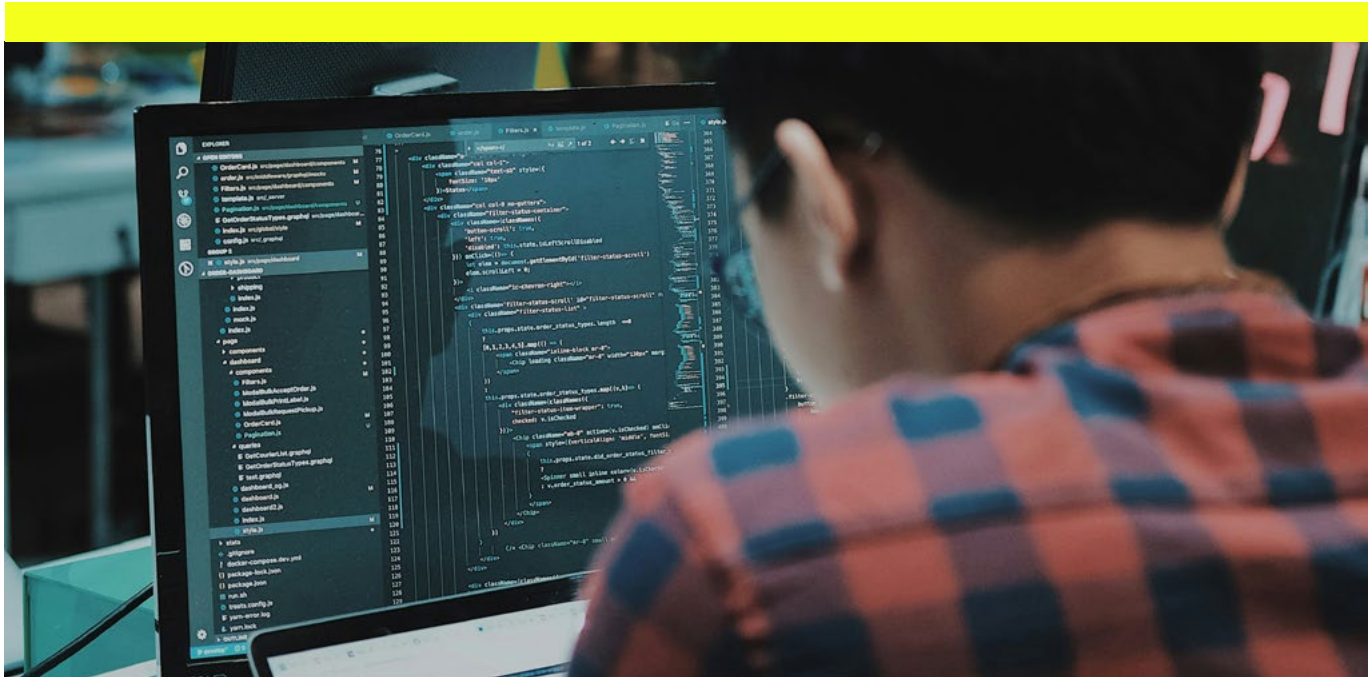
- External (100%) (breaches)

Actor motives

- Financial (95%)
- Espionage (5%) (breaches)

Data compromised

- Credentials (50%)
- Personal (41%)
- Internal (20%)
- Other (14%) (breaches)



Phishing in the wind

There are a lot of vectors on which we need to educate our employees and end users, and we're positive that in another five years, there will be new ones that we will have to add to our list. However, even with the growth of these new vectors and types of attacks, we tend to see the core social tactics such as Pretexting and Phishing still being used often (Figure 8). More than 40% of incidents involved Pretexting, and 31% involved Phishing. Other tried-and-true tactics such as attacks coming in via email, text and websites (Figure 9). Regardless of the exact method that attackers use to reach organisations, the core tactic is the same: They seek to exploit our human nature and our willingness to trust and be helpful for their own gain. While these attacks all share that commonality, one rather significant difference is the scale and pervasiveness of these tactics.

First, the good news. We have not seen a dramatic rise in Pretexting like we did last year. However, it is also true that it hasn't decreased but instead has maintained its position as the top type of Social Engineering incident. As a quick reminder, when we talk about Pretexting, largely consider this as a stand-in for BEC (Business Email Compromise), where attackers leverage existing email chains to convince victims to do something, such as update an associated bank account with a deposit.

Low tech, high cost

Unfortunately, the bad news comes next, which is that BECs continue to have a substantial financial impact on organisations. There isn't any growth this year as compared to last year, but nor has it decreased, with the median transaction hovering around $50,000.

One of the best things you can do when you realise you are a victim of BEC fraud is to promptly work with law enforcement. From the cases our data contributors at the FBI IC3 have worked, they were able to recoup 79% or more of the losses in half of the cases. On the less fortunate side, 18% of the incidents had nothing frozen and potentially lost everything that was sent to the criminals.

I hope this threat finds you well.

Social attacks, such as those involving Phishing, have long played their part in ushering in a ransomware deployment, as typified by the leveraging of those techniques in the ALPHV breach of MGM Resorts and other entertainment groups. But given the shift in tactics by some groups, along with the Extortion action being the result of the breach as opposed to an initial one, this seemingly "System intrusion-y" attack now also shows up in this pattern. Keep in mind, however, that Extortion isn't anything new in this pattern. We've seen various iterations of it from the empty threats ("We've hacked your phone and caught you doing NSFW stuff.") to somewhat credible threats ("Look us up. We're super-duper hackers that'll DDoS you.") to very credible threats ("We'll leak the data we took. Here are samples for you to validate."). This year, however, Extortion showed up in spades because of the MOVEit breach, which affected organisations on a relatively large scale and in an extremely public fashion.

There has been a dramatic increase in compromising servers via Hacking. Given the prevalence of these types of attacks, we recommend discussions with leadership to determine what the course of action should be if they occur in your organisation.

School of phishes

This is probably cliché at this point, but we're believers that the first line of defence for any organisation isn't the castrametation (camp layout) of their systems but the education of their key staff, including end users.

Fortunately, this isn't simply us standing on our "user-awareness" soapbox. We have both figures and hard numbers to help quantify our stance. The first lesson to learn is that Phishing attacks happen fast. The median time to click on a malicious link after the email is opened is 21 seconds, and then it takes only another 28 seconds to enter the data. That leads to a frightening finding: The median time for users to fall for phishing emails is less than 60 seconds. Some good news is that we seem to be getting better regarding phishing test reporting. More than 20% of users identified and reported phishing per engagement, including 11% of the users who did click the email. This is another impressive improvement and one that we desperately need to catch up with the previous year's increases in Phishing and Pretexting.

Controls for consideration

There are a fair number of controls to consider when confronting this complex threat, and all of them have pros and cons. Due to the strong human element associated with this pattern, many of the controls pertain to helping users detect and report attacks as well as protecting their user accounts if they fall victim to a phishing attack. Lastly, due to the importance of the role played by law enforcement in responding to BECs, it is key to have plans and contacts already in place.

Protect accounts

Account Management [5]

- Establish and Maintain an Inventory of Accounts [5.1]
- Disable Dormant Accounts [5.3]

Access Control Management [6]

- Establish an Access Granting/ Revoking Process [6.1, 6.2]
- Require MFA for Externally-Exposed Applications [6.3]
- Require MFA for Remote Network Access [6.4]

Security awareness programmes

- Security Awareness and Skills
- Training [14]
- Although not part of the CIS Controls, a special focus should be placed on BEC and processes associated with updating bank accounts

Managing incident response

Incident Response Management [17]

- Designate Personnel to Manage Incident Handling [17.1]
- Establish and Maintain Contact Information for Reporting Security Incidents [17.2]
- Establish and Maintain an Enterprise Process for Reporting Incidents [17.3]

Impact of Social Engineering on Manufacturing

Brunswick Corporation, a leading marine manufacturer, was hit by a cyberattack involving social engineering tactics such as phishing. This attack led to the shutdown of multiple manufacturing plants, resulting in an estimated $85 million in losses. The incident highlights the severe impact of social engineering on the manufacturing sector, where such attacks can disrupt operations, lead to significant financial losses, and underscore the urgent need for stronger cybersecurity measures and employee vigilance.

Source: https://www.itpro.com/technology/artificial-intelligence-ai/370366/social-engineering-attacks-generative-ai-soar-135

04. Supply Chain

The weakest links in the chain of interconnection

As the growth of exploitation of vulnerabilities and software supply chain attacks make them more commonplace in security risk register discussions, we would like to suggest a new third-party metric where we embrace the broadest possible interpretation of the term. We calculated a supply chain interconnection influence in 15% of the breaches we saw, a significant growth from 9% last year. A 68% year-over-year growth is solid, but what do we mean by this? For a breach to be a part of the supply chain interconnection metric, it will have taken place because either a business partner was the vector of entry for the breach (like the now fabled heating, ventilating and air-conditioning [HVAC] company entry point in the 2013 Target breach) or if the data compromise happened in a third-party data processor or custodian site (common in the MOVEit cases, for instance).

Less frequently found in our dataset, but also included, are physical breaches in a partner company facility or even partner vehicles hijacked to gain entry to an organisation's facilities.

So far, this seems like a standard third-party breach recipe, but we are also adding cases, such as SolarWinds and 3CX, in which their software development processes were hijacked, and malicious software updates were pushed to their customers to be potentially leveraged in a second step escalation by the threat actors. Those breaches are ultimately caused by the initial incident in the software development partner, and so we are adding those to this tab.

Now for the controversial part: Exploitation of vulnerabilities is counted in this metric as well. As much as we can argue that the software developers are also victims when vulnerabilities are disclosed in their software (and sure, they are), the incentives might not be aligned properly for those developers to handle this seemingly interminable task. These quality control failures can disproportionately affect the customers who use this software. We can clearly see what powerful and wide-reaching effects a handful of zero-day or mismanaged patching rollouts had on the general threat landscape. We stopped short of adding exploitation of misconfigurations in installed software because, although those could be a result of insecure defaults, system admins can get quite creative sometimes.

Figure 10 (right) shows the breakdown of VERIS actions in the supply chain metric and as expected, it is driven by Exploit vuln, which ushers Ransomware and Extortion attacks into organisations. This metric ultimately represents a failure of community resilience and recognition of how organisations depend on each other. Every time a choice is made on a partner (or software provider) by your organisation, and it fails you, this metric goes up.

We recommend that organisations start looking at ways of making better choices to not reward the weakest links in the chain. In a time where disclosure of breaches is becoming mandatory, we might finally have the tools and information to help measure the security effectiveness of our prospective partners.

We will keep a close watch on this one and seek to improve its definition over time. We welcome feedback and suggestions of alternative angles, and we believe the only way through it is to find ways to hold repeat offenders accountable and reward resilient software and services with our business.

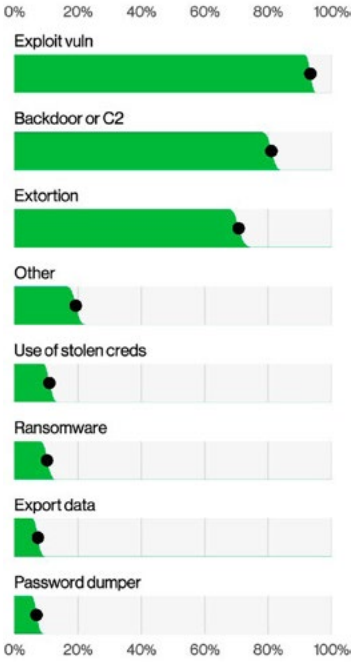


Figure 10. Action varieties in selected supply chain interconnection breaches (n=1,075)

Violence-as-a-Service (VaaS)

This is an emerging trend where cybercriminals employ physical intimidation tactics to coerce businesses into paying fees, often in conjunction with ransomware attacks. While our insight into VaaS is still developing, our Threat Intelligence service has confirmed an increase in such incidents.

Other topics for discussion

We are only human after all

One other combined metric we have been tracking for a few years is related to the human element in breaches. There is a lot of focus on how fully automated attacks can ruin an organisation's day, but it is often surprising how much the people inside the company can have a positive effect on security outcomes.

This year, we have tweaked our human element metric a bit, so its impact and action opportunities are clearer. You see, when DBIR authors (and the whole industry in general) would discuss this metric, it would be alongside an opportunity gap for security training and awareness. It is not perfect, but if you had a clear investment path that could potentially improve the outcomes of more than two-thirds of potential breaches, you might at least sit down and listen. It turns out that our original formula for what was included in the human element metric built in Privilege Misuse pattern breaches, which are the cases involving malicious insiders. Having those mixed with honest mistakes by employees did not make sense if our aim was to suggest that those could be mitigated by security awareness training the new human element over time (with malicious insiders removed) to provide a better frame of reference for our readers going forward. It is present in more than two-thirds of breaches, more precisely in 68% of breaches.

Artificial general intelligence threat landscape, emphasis on "artificial", not "intelligence"

This is still a very timely topic and one that has been occupying the minds of technology and cybersecurity executives worldwide.

We did keep an eye out for any indications of the use of the emerging field of generative artificial intelligence (GenAI) in attacks and the potential effects of those technologies, but nothing materialised in the incident data we collected globally. After performing text analysis alongside our criminal forums data contributors, we could obviously see the interest in GenAI (as in any other forum, really), but the number of mentions of GenAI terms alongside traditional attack types and vectors such as "phishing", "malware", "vulnerability" and "ransomware" were shockingly low, barely breaching 100 cumulative mentions over the past two years.

Most of the mentions involved the selling of accounts to commercial GenAI offerings or tools for AI generation of non-consensual pornography.

If you extrapolate the commonly understood use cases of GenAI technology, it could potentially help with the development of phishing, malware and the discovery of new vulnerabilities in much the same way it helps your Year 11 student write that book report for school, or your average AI social media influencer pretend to create a website by taking a picture of a drawing on a napkin.

But would this kind of assistance really move the needle on successful attacks? One can argue, given our Social Engineering pattern numbers from the past few years, that Phishing or Pretexting attacks don't need to be more sophisticated to be successful against their targets. We have seen with the growth of BEC-like attacks. Similarly, malware, especially of the Ransomware flavour does not seem to be lacking in effectiveness, and threat actors seem to have a healthy supply of zero-day vulnerabilities for initial infiltration into an organisation.

From our perspective, the threat actors might well be experimenting and trying to come up with GenAI solutions to their problems. There is evidence being published of leveraging such technologies in "learning how to code" activities by known state-sponsored threat actors. But it really doesn't look like a breakthrough is imminent or that any attack-side optimisations this might bring would even register on the incident response side of things. The only exception here has to do with the clear advancements on deepfake-like technology, which has already created a good deal of reported fraud and misinformation anecdotes.

We hope that you have found this personalised snapshot of the 2024 DBIR useful. The full report has masses of additional insight. And the DBIR is just one of our many security publications. Our threat intelligence team and numerous security practitioners publish thought leadership on many topics—some of which can be found here.

We'd be very pleased to discuss any of these topics further with Nestlé. In the first instance, please speak to a member of your Verizon account team.

verizon business