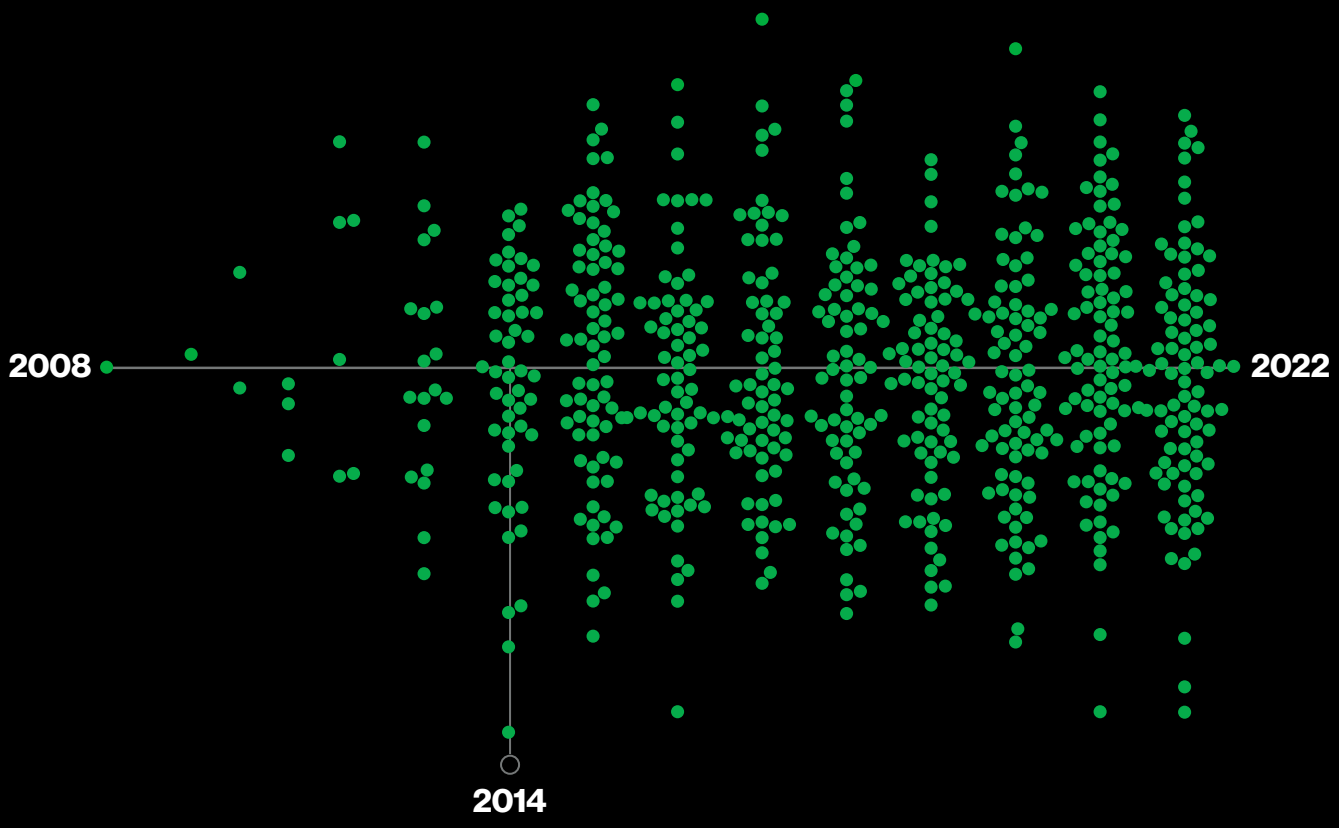

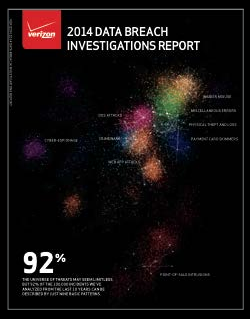

4 Industries

Introduction

If you are a long-time reader this introduction may be redundant, but for new readers it is worth perusing. This year we looked at 23,896 incidents, which boiled down to 5,212 confirmed data breaches. As always, we break these incidents and breaches into their respective industries to illustrate that all industries are not created equal. At least not when it comes to attack surfaces and threats. The type of attacks suffered by a particular industry will have a great deal to do with what infrastructure they rely upon, what data they handle and how people (customers, employees and everyone else) interact with them.

A large organization whose business model focuses entirely on mobile devices where their customers use an app on their phone will have different risks than a small Mom and Pop shop with no internet presence, but who use a point-of-sale vendor that manages their systems for them. The infrastructure, and conversely the attack surface, largely drives the risk.

Therefore, we caution our readers not to make inferences about the security posture (or lack thereof) of a particular sector based on how many breaches or incidents their industry reports. These numbers are heavily influenced by several factors, including data breach reporting laws and partner visibility. Because of this, some of the industries have very low numbers, and as with any small sample, we must caution readers that our confidence in any statistics derived from a small number must also be less.

When examining industries with a small sample, we will provide ranges where the actual value may reside. This allows us to maintain our confidence interval while giving you an idea of what the actual number might be, given a large enough sample. For example, instead of stating "In the Accommodation industry, 92% of attacks were financially motivated," we might state that "financially motivated attacks ranged between 86% and 100%." Check out our riveting Methodology section for far more information about the statistical confidence background used throughout this report.

If you are reading this only for a glimpse of your industry, our recommendation is to verify what the top patterns are on the summary table accompanying each industry and also spend some time with those pattern sections. In addition, we provide a description of what Center for Internet Security (CIS) Critical Security Controls) to prioritize in each industry section for ease of reading if you want to get straight to strategizing your security moves.

	Incidents				Breaches			
Industry	Total	Small (1-1,000)	Large (1,000+)	Unknown	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	23,896	2,065	636	21,195	5,212	715	255	4,242
Accommodation (72)	156	2	1	153	69	1	1	67
Administrative (56)	39	5	7	27	19	3	5	11
Agriculture (11)	243	1	1	241	39	1	0	38
Construction (23)	127	21	7	99	57	8	5	44
Education (61)	1,241	112	48	1,081	282	57	15	210
Entertainment (71)	215	12	5	198	96	6	3	87
Finance (52)	2,527	103	50	2,374	690	56	32	602
Healthcare (62)	849	36	14	799	571	14	10	547
Information (51)	2,561	59	25	2,477	378	27	10	341
Management (55)	8	1	2	5	2	0	0	2
Manufacturing (31-33)	2,337	168	74	2,095	338	54	22	262
Mining (21)	231	0	0	231	132	0	0	132
Other Services (81)	180	16	1	163	101	8	1	92
Professional (54)	3,566	1,095	144	2,327	681	263	52	366
Public Administration (92)	2,792	110	88	2,594	537	74	25	438
Real Estate (53)	118	31	5	82	76	19	2	55
Retail (44-45)	629	157	68	404	241	54	35	152
Transportation (48-49)	305	26	38	241	137	17	23	97
Utilities (22)	172	20	14	138	47	14	3	30
Wholesale Trade (42)	166	79	33	54	68	38	8	22
Unknown	5,434	11	11	5,412	651	1	3	647
Total	23,896	2,065	636	21,195	5,212	715	255	4,242

Table 2. Number of security incidents and breaches by victim industry and organization size

Breaches

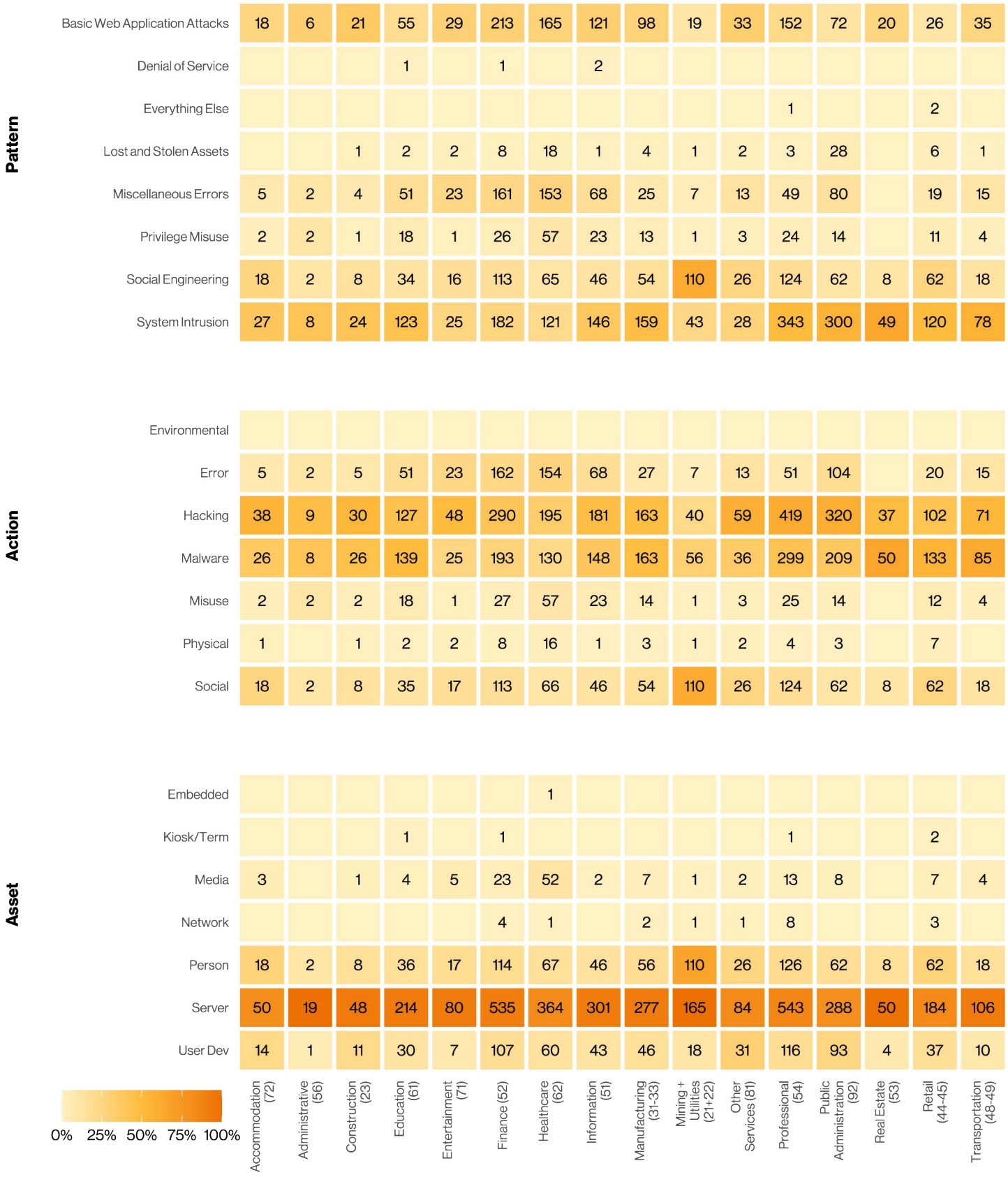

Figure 75. Breaches by industry

Incidents

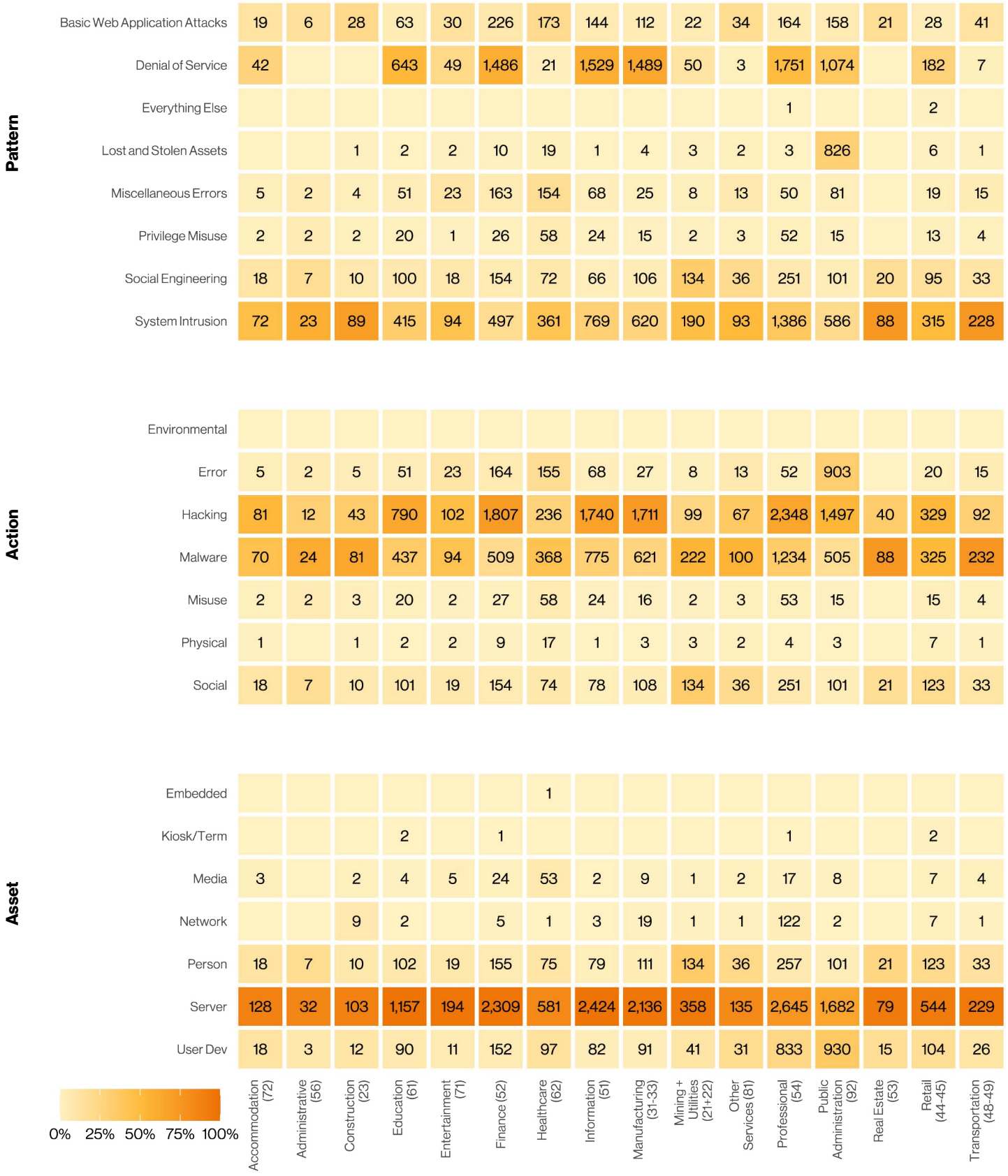

Figure 76. Incidents by industry

Accommodation and Food Services NAICS 72

Frequency	156 incidents, 69 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 90% of breaches
Threat actors	External (90%), Internal (10%) (breaches)
Actor motives	Financial (91%), Espionage (9%) (breaches)
Data compromised	Credentials (45%), Personal (45%), Payment (41%), Other (18%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be targeted by financially motivated criminals going after Payment and Personal data.

Summary

Accommodation and Food Services, while having seen a decrease of System Intrusion since 2016, is still victimized by Malware via email and the Use of stolen credentials used against Web application.

Patterns in years	5-year difference	3-year difference	Difference with peers
System Intrusion	Less	Less	No change
Social Engineering	Greater	No change	No change
Basic Web Application Attacks	Greater	Greater	No change

The Accommodation and Food Services industry is one of the few industries that saw a drop in terms of System Intrusion. However, it shows similar trends to other industries in regard to Basic Web Application Attacks and Social Engineering. They have been on the increase over the last 5 years, and are now a bit closer to the same baseline for the types of attacks that the other industries are experiencing.

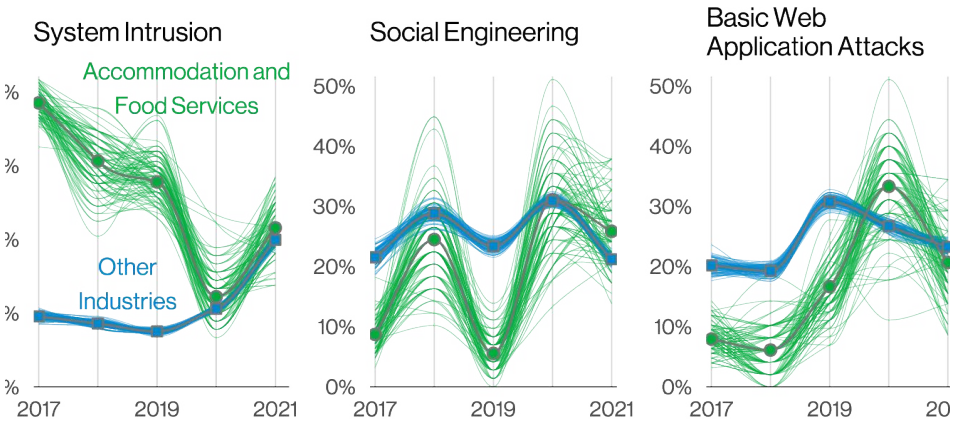

Figure 77. Top patterns over time in Accommodation and Food Services breaches

Figure 78 captures the top Action varieties found in this industry. This is one of the few industries that is extremely long tailed, with over 80% of the breaches including Actions not captured in the top five varieties. While that might seem imposing, keep in mind that the vectors are still the usual suspects found in the other industries: Email, Web apps and Desktop sharing software.

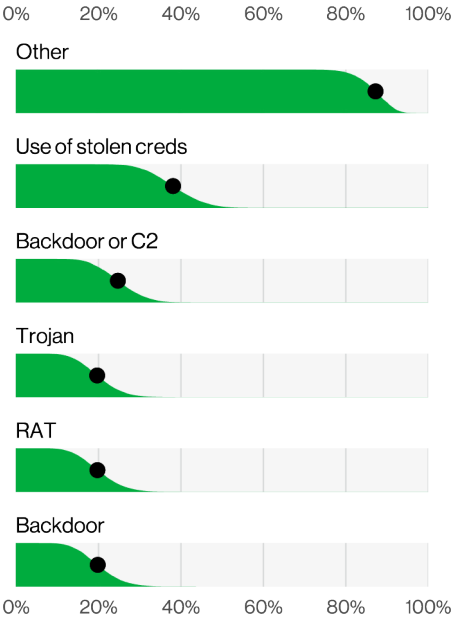

Figure 78. Top Action varieties in Accommodation and Food Services breaches (n=58)

Looking back
In the 2012 DBIR, Accommodation and Food Services represented over 54% of our cases and has since dropped to less than 2% of our incidents. This represents both a total drop in cases but also a rather dramatic drop in incidents and may be representative of a larger shift in the criminal ecosystem to target and victimize not only the organizations with credit card data but any organization.

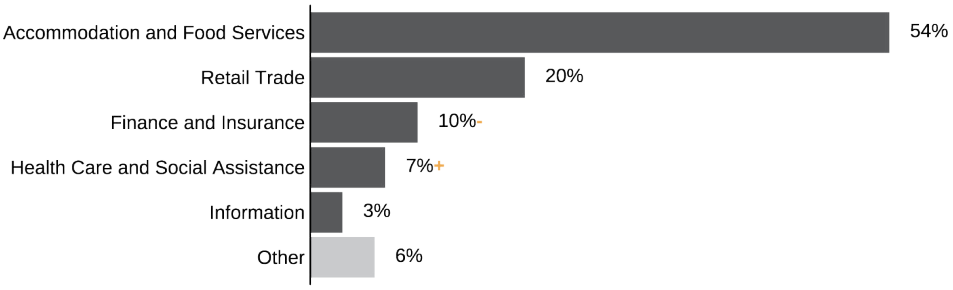

Figure 79. Industry groups represented by percent of breaches (2012 DBIR Figure 3)

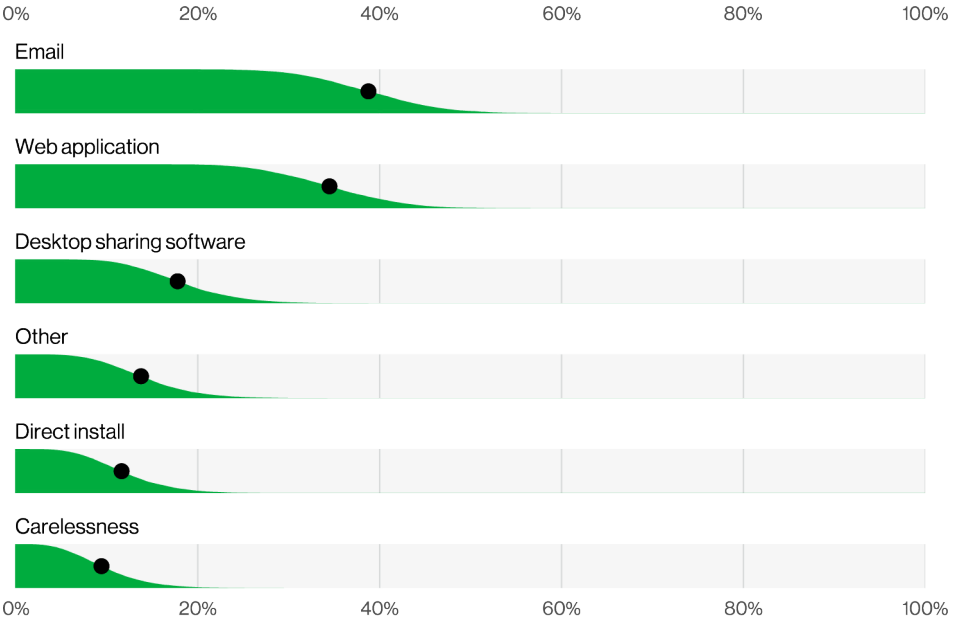

Figure 80. Top Action vectors in Accommodation and Food Services breaches (n=47)

Arts, Entertainment and Recreation NAICS 71

Frequency	215 incidents, 96 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Errors represent 80% of breaches
Threat actors	External (74%), Internal (26%) (breaches)
Actor motives	Financial (97%), Grudge (3%) (breaches)
Data compromised	Personal (66%), Credentials (49%), Other (23%), Medical (15%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The patterns are the same, but the order is not. Medical data continues to be compromised in this industry.

Summary

The System Intrusion and Basic Web Application Attacks patterns exchanged positions, but the Miscellaneous Errors pattern held on to 3rd place on the podium. For incidents, Denial of Service attacks remain a problem in the sector, particularly for the Gambling industry.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	No change
System Intrusion	No change	No change	Less
Miscellaneous Errors	No change	No change	Greater

This industry mainly covers live performances, and whether dance, theater or sporting events, the common thread is that none are pre-recorded for later broadcast. It also includes the gambling industry. One can only imagine the different attack surfaces that are present for the myriad organization types belonging to this NAICS code. Something many of them have in common, however, is that at least a portion of their infrastructure relies on the internet to perform critical functions, whether that is ticket sales or taking orders (or bets as the case may be). In any event, when a Denial of Service attack comes calling, it is a very unwelcome guest. Nevertheless, it is a frequent guest in this sector (particularly in the Gaming organizations in the APAC region), and represents over 20% of incidents.

With regard to breaches, the three patterns listed in the At-a-Glance table show the vulnerability of the infrastructure beyond disruption of services. Once the attackers get in, they can wreak havoc in earnest. These attackers are largely External actors, with a Financial motive, although there are a small amount of Grudge-motivated attacks in this sector as well.

The inclusion of the Basic Web Application Attacks is concerning, given the less complex nature of these attacks. Conversely, the attackers have to try much harder to gain their prize in the System Intrusion attacks, where ransomware is always a favored tool. As we have seen in the past, every attacker loves credentials, and will use them to masquerade as a legitimate employee to evade capture for as long as it takes to get what they are after.

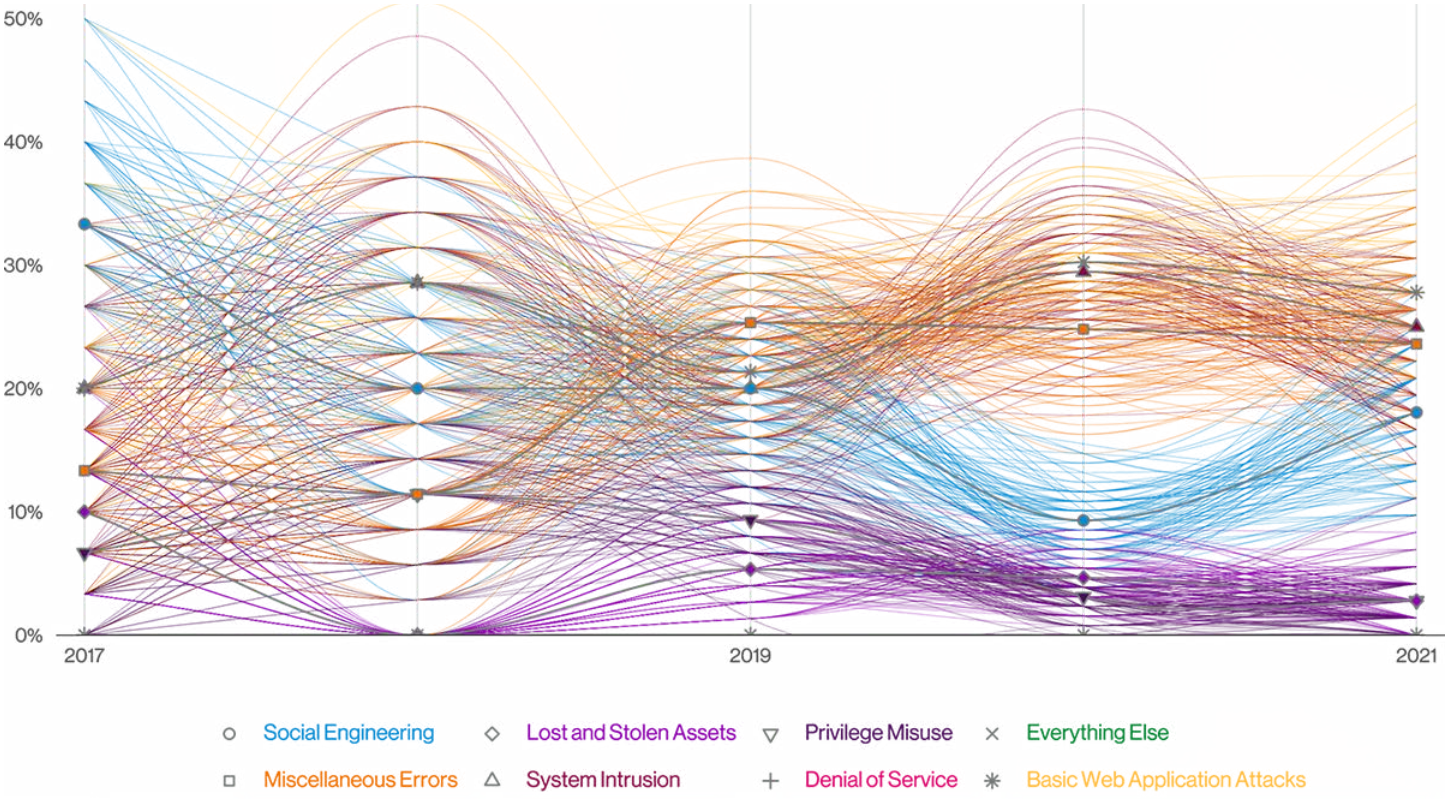

Figure 81. Patterns over time in Arts and Entertainment breaches

The most commonly taken data is Personal information (although it is down from a high last year of 83%) and Credentials. Oddly enough, Medical data is still being snarfed up (technical term) in 15% of the breaches in this sector. This was similar to last year (at 26%), but it remains a puzzling data type to find in a sector that has no medical affiliation. It may be that the data taken is from companies that are self-insured for their employee medical needs, and so have a need to store that kind of data, or it could possibly be from some form for Workers Compensation data (on the job injuries). Additionally, this NAICS code includes sports teams which could account for a certain number of stolen medical records. Regardless, it is a rather counterintuitive finding.

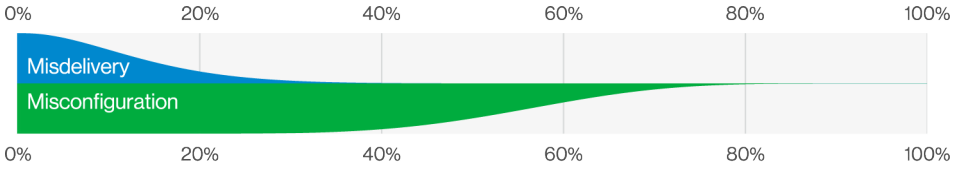

Figure 82. Misdelivery vs Misconfiguration in Arts and Entertainment industry Error breaches (n=16)

Miscellaneous Errors remain in the top three patterns again this year (25%). The Misconfiguration error was the most common, representing approximately 15% of the breaches. It appears this sector simply traded one problem for another as Misdelivery errors (the most common last year) have dropped considerably.

Educational Services NAICS 61

Frequency	1,241 incidents, 282 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 80% of breaches
Threat actors	External (75%), Internal (25%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (63%), Credentials (41%), Other (23%), Internal (10%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be impacted by attacks targeting their external infrastructure and are largely targeted by External actors with Financial motives. However, Educational Services also faces errors as one of the top causes of breaches.

Summary

Educational Services follows an eerily similar trend to the majority of the other industries; it is experiencing a dramatic increase in Ransomware attacks (over 30% of breaches). In addition, this industry needs to protect itself against stolen credentials and phishing attacks potentially exposing the personal information of its employees and students.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
System Intrusion	Greater	Greater	Greater
Miscellaneous Errors	No change	Less	Greater

Alright, class is back in session, put away your NSYNC Trapper Keeper and get out a number two pencil, cause you're about to get schooled on the breaches and incidents impacting the Educational Services industries. System Intrusion, Social Engineering and DoS are the leading causes of incidents and System Intrusion, BWAA and Errors lead the way with regard to breaches. Falling along the peak of the grading curve, this industry also has Use of stolen creds and Ransomware as the top two action varieties, which is a very dangerous combination. The rumor is stolen creds and ransomware quit school due to recess, because they don't play around.

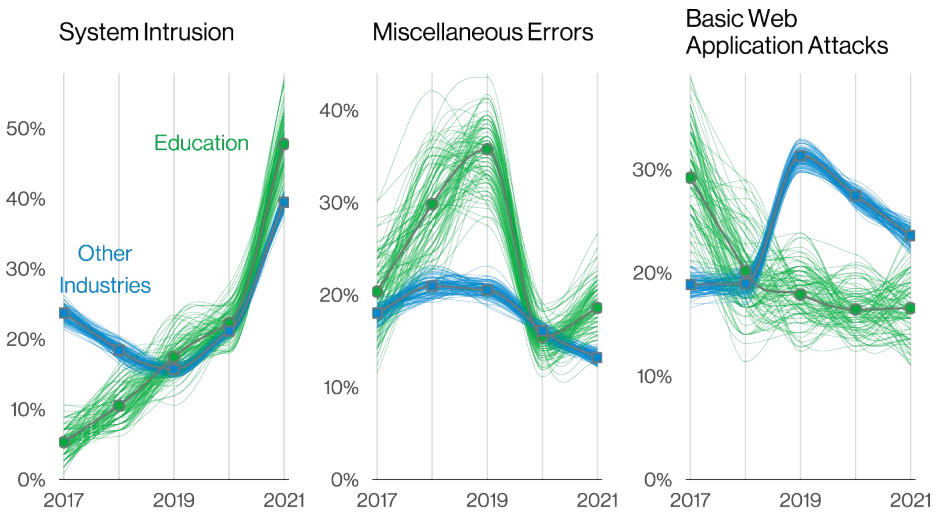

Figure 83. Top patterns over time in Education breaches

While an erroneous number in a calculation might result in a few points off of your homework, the erroneous end user might result in a data breach. Thirty four percent of the errors found in this industry were from an email sent to the wrong people, or with the wrong attachment.

While errors may have decreased over the past three years, they're still a relatively normal occurrence that should be taken seriously, especially considering the various troves of data schools handle, we would hate to have our poor little Bobby Tables' data leaked.[25]

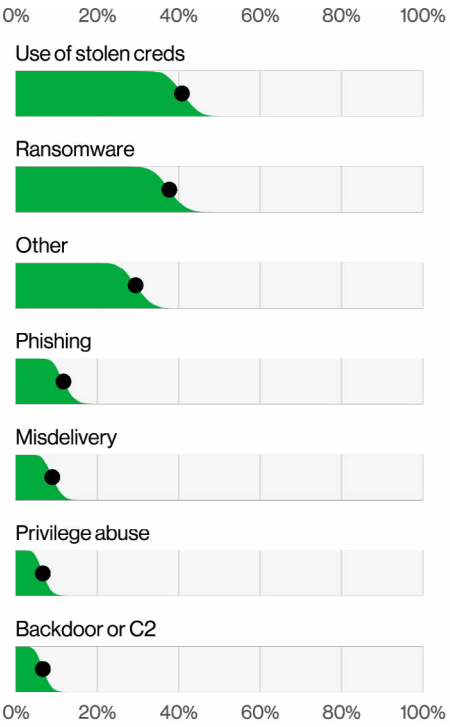

Figure 84. Top Action varieties in Educational Services breaches (n=218)

2017 Yearbook

There's nothing quite like the feeling of nostalgia that hits you when you're looking over your old yearbook. Signatures and notes from friends long ago, ahh, the good old days. We get that same feeling when looking back at the 2017 DBIR and see Cyber-Espionage as the top breach pattern for this industry. No worries though, Espionage has not graduated and moved away yet. It shows up in 34% of incidents this year. Figure 85 captures the shifts in data and the somewhat dramatic rise of Espionage that is still all too present today. Unfortunately, unlike your opinionated high school friends on social media, you can't just block espionage from cluttering up your feed.

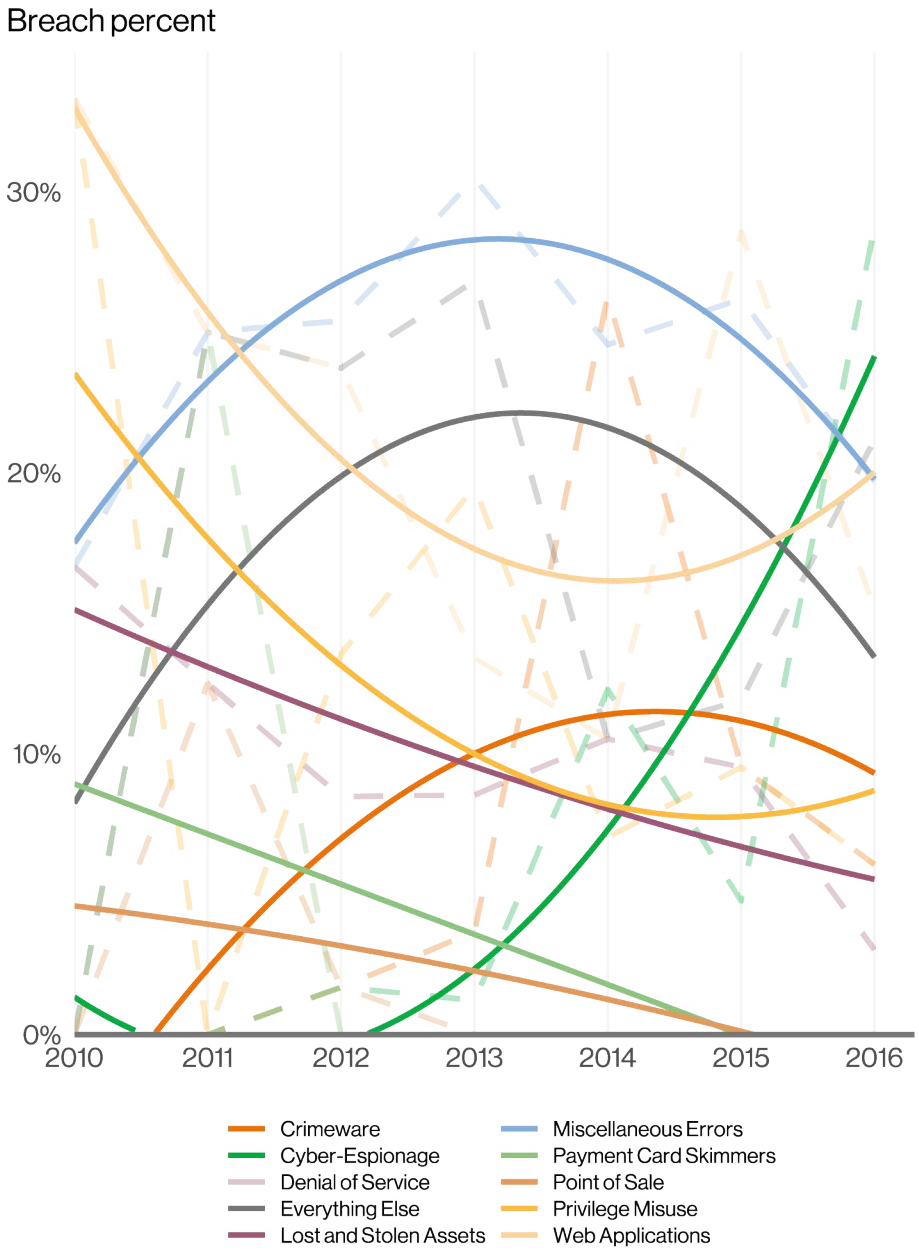

Figure 85. Percent of breach classification patterns over time within the Education industry (DBIR 2017 Figure 17)

25 https://xkcd.com/327, a classic.

Financial and Insurance NAICS 52

Frequency	2,527 incidents, 690 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Error represent 79% of breaches.
Threat actors	External (73%), Internal (27%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (71%), Credentials (40%), Other (27%), Bank (22%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Data Protection (CSC 3)
What is the same?	Basic Web Application Attacks and Miscellaneous Errors continue to play a large part in breaches for this vertical as they did last year.

Summary

The Financial sector continues to be victimized by financially motivated organized crime, often via the actions of Social (Phishing), Hacking (Use of stolen credentials) and Malware (Ransomware). Finally, Miscellaneous Errors, often in the form of Misdelivery, is still very common as it has been for the past three years in a row.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Less
System Intrusion	Greater	Greater	Greater
Miscellaneous Errors	Greater	Greater	Greater

In 2016 servers were involved in 50% of Financial breaches, as opposed to 90% currently. However, the specific variety of "Server–Web application" has increased from 12% to 51% over that same timeframe, thus accounting for Basic Web application Attacks' position in the top three patterns. A key component of these attacks is that they usually involve the Use of stolen credentials, which is the number one Action variety in this vertical. These creds may have been obtained in any number of ways, but brute force hacking and credential stuffing are the most likely culprits. One thing is certain, stolen creds and web apps go together like peanut butter and chocolate.

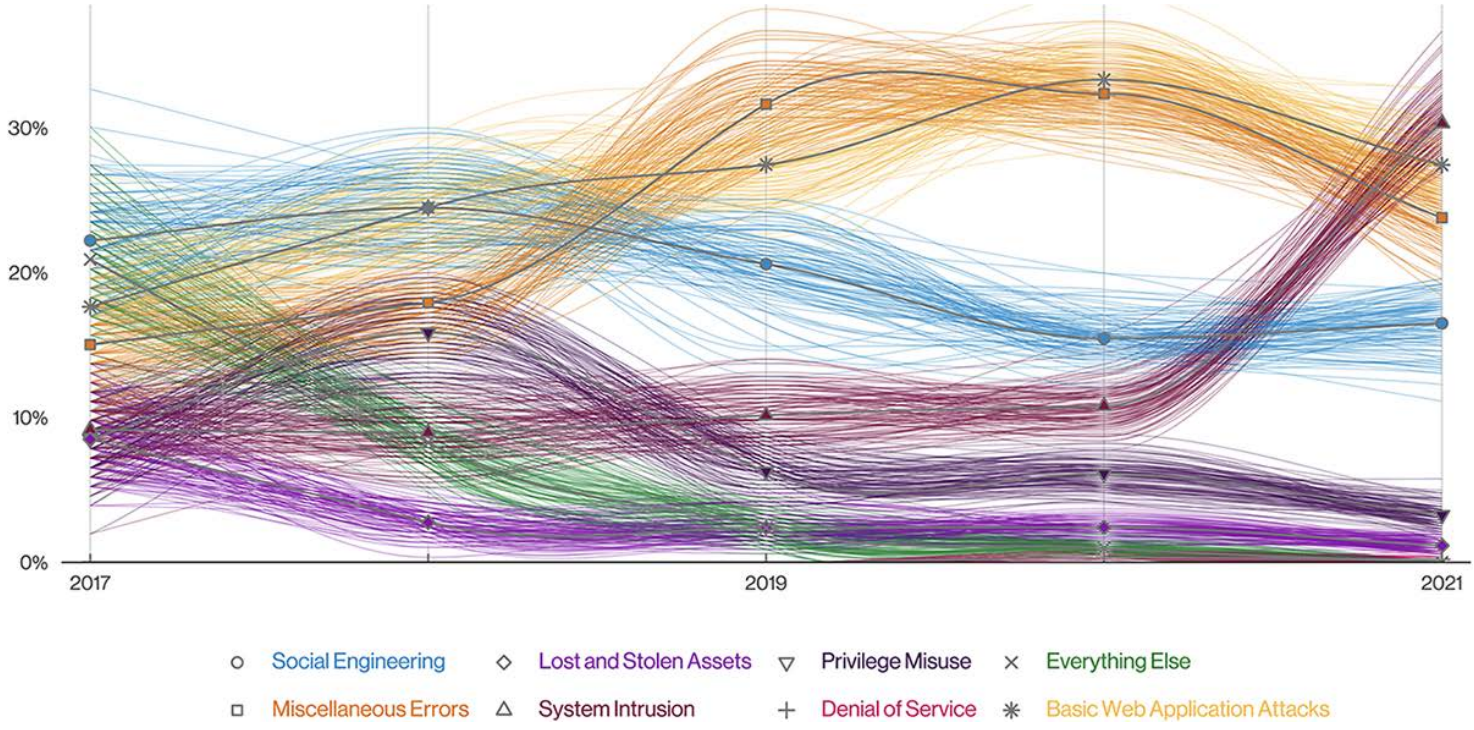

Figure 86. Patterns over time in Financial and Insurance industry breaches

"I'll show you mine if you show me yours"

The Error variety of "Misdelivery" (16%) is the second most common action variety in this vertical. Misdelivery is exactly what it sounds like, delivering PII or other sensitive information to the wrong recipient. One might expect to see that variety more often in Public Sector or Healthcare because, by their very nature, they send a great deal of mail. Instead, our data indicates that Misdelivery is approximately three times higher in Financial than in the other industries. We here on the DBIR team were taken aback by this finding, as it would be embarrassing if any unauthorized person were to view our checks and learn that we make countless millions for writing this report each year.[26]

"Through the years..."

System Intrusion has doubled from 14% in 2016 to 30% this year. Organized crime was responsible for only 49% of breaches in 2018 vs the 79% we see in this report. Availability was affected in only 6% of breaches back in 2016, vs 14% today, and the discovery method of Actor disclosure was 5% (in 2016) as opposed to the 58% in this year's report. We need hardly say that this is mainly due to ransomware attacks, but to be on the safe side, we will say it anyway:

This is mainly due to ransomware attacks. As long as ransomware continues to be a high profit, low risk attack, criminals will continue to utilize it.

Finally, we would be remiss if we did not mention that DoS attacks continue to be a huge problem and account for 58% of security incidents in this vertical. That is approximately twice as much as we see in the other industries.

26 If only.

Healthcare NAICS 62

Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches
Threat actors	External (61%), Internal (39%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The top three patterns are the same, but the order is not. The threat actors were exactly the same as last year (down to the percentage point).

Summary

The Basic Web Application Attacks have overtaken the Miscellaneous Errors in causing breaches in this sector. Errors are still a significant problem.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Greater
System Intrusion	Greater	Greater	Less
Miscellaneous Errors	Less	Less	Greater

Insiders? What Insiders?

Healthcare is the industry where the internal actor has figured prominently in breaches since we first began collecting and reporting data. While the make-up of the insider breach has moved from being largely malicious Misuse incidents to the more benign (but no less reportable) Miscellaneous Errors, we have always been able to rely on this industry to tell the insider threat story. With the rise of the Basic Web Application Attacks pattern in this vertical, those inside actors no longer hold sway. Move over Insiders, the big dogs are here.

Make no mistake (no pun intended) your employees are still causing breaches, but they are more than 2.5 times more likely to make an error than to maliciously misuse their access. Misdelivery and Loss are the most common errors (and they are so close, we'd need a photo finish to determine a winner).

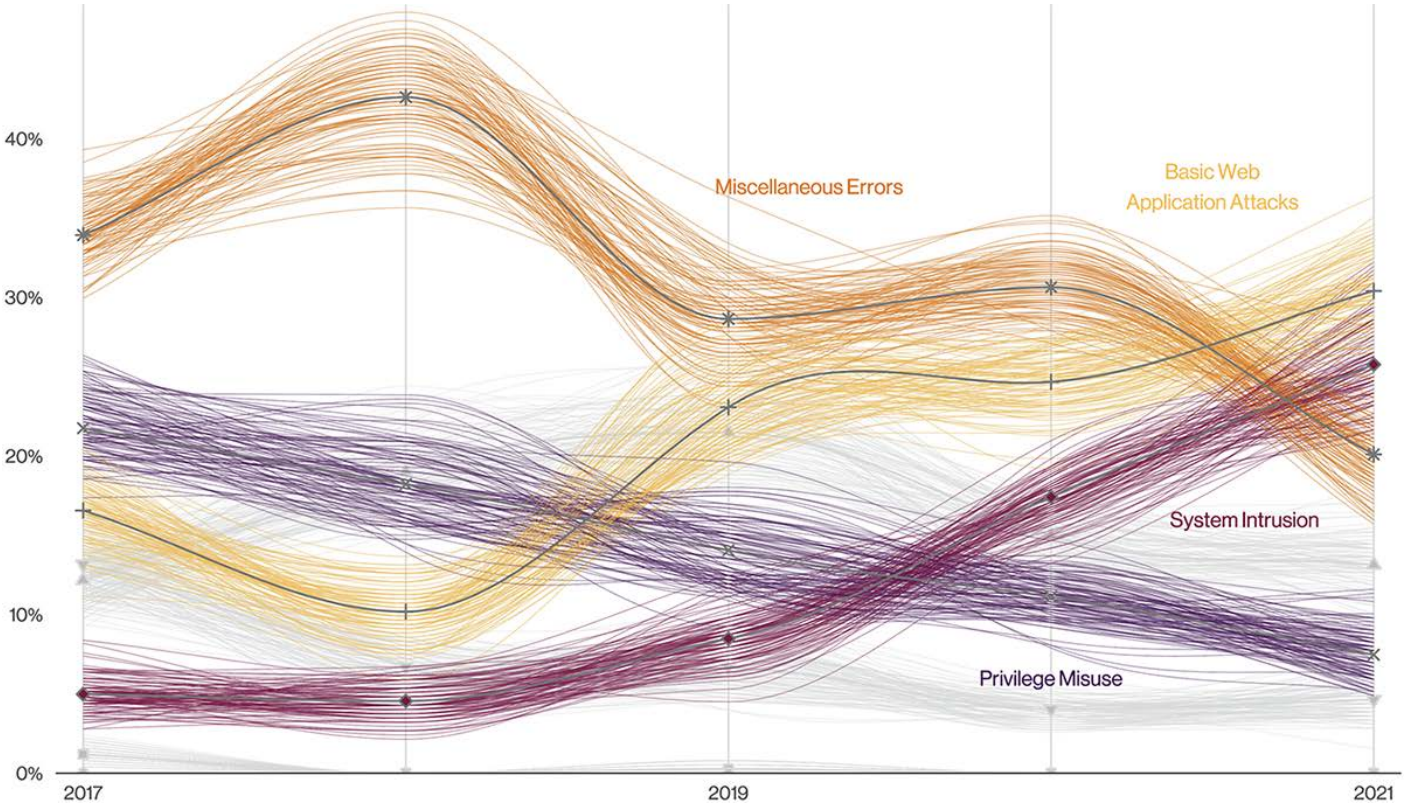

Figure 87. Patterns over time in Healthcare industry breaches

Figure 87 illustrates the change over time in patterns for Healthcare. Back in 2015, the top pattern was Privilege Misuse, followed by Miscellaneous Errors. It wasn't until 2019 that we started to see the rise of Basic Web Application Attacks, and they have clearly become a serious problem for everyone, not just this industry. Healthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns (both from the System Intrusion pattern, which came in third). With the increase in ransomware, comes the associated increase of the discovery method of Actor Disclosure. It is a bad day when that ransom note pops up after the encryption has been triggered, providing convenient methods of payment for these customer service-focused threat groups. (And really, who doesn't want to make it easy for their "customers" to pay them?)

For the second year, Personal data is compromised more often than Medical. Do we consider this the norm now for the one industry with a plethora of medical data? Is this because the actors are just getting in and getting their encryption game on without regard to the type of records they are rendering inaccessible? Only those in the industry know for certain if they have increased their controls around their Medical data but left Personal data in the waiting room.

Information

NAICS 51

Frequency	2,561 incidents, 378 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 81% of breaches
Threat actors	External (76%), Internal (24%) (breaches)
Actor motives	Financial (78%), Espionage (20%), Ideology (1%), Grudge (1%) (breaches)
Data compromised	Personal (66%), Other (35%), Credentials (27%), Internal (17%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	Surprisingly, over the last five years Social breaches have remained roughly the same. This may be because Social breaches are targeting customers resulting in Hacking breaches (which have also stayed pretty level) to the company due to stolen credentials.

Summary

System Intrusion moves ahead of Errors and Basic Web Application Attacks to claim the top spot this year in breaches, meanwhile DDoS maintains its top position in incidents. Malware has seen a noticeable rise over the past two years, while Errors appear to be on the down swing since their rise five years ago.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	Greater
Miscellaneous Errors	Greater	Less	Greater
System Intrusion	Greater	Greater	Greater

Last year, not unlike your boss at your last performance review, we highlighted the Errors in the Information industry. However, as we can see in Figure 88, there has been clear progress that we can put on the mid-year review. Errors have experienced a decline since their upswing half a decade ago in 2017.

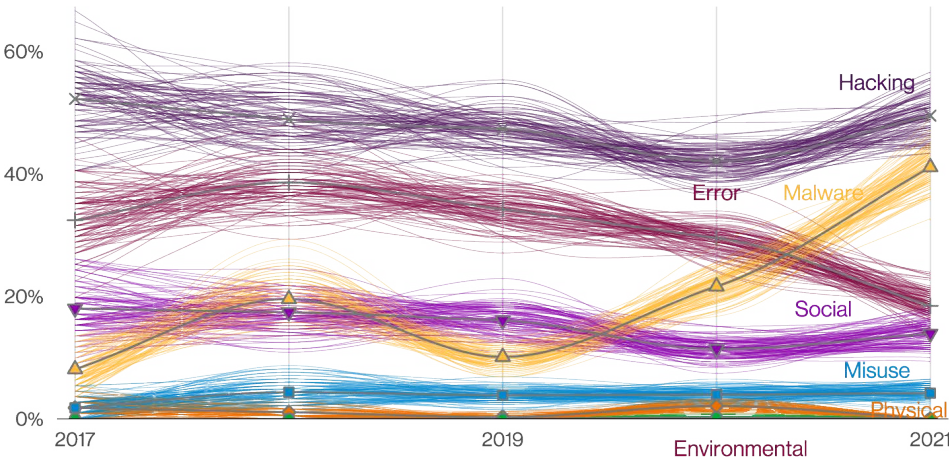

Figure 88. Actions over time in Information industry breaches

To maintain the balance however, Malware has seen a measurable increase over the past two years. That is reflected in Figure 89. System Intrusion has jumped to the top in this vertical, even rising above Basic Web Application Attacks.

One interesting effect of having System Intrusion in the number one position is that the Information industry contains a smorgasbord of Action varieties. Use of stolen creds is the most common, but after that, a legion of varieties are present, with Ransomware, Misconfiguration, Backdoor or C2, and Export Data appearing in more than 4% of breaches. In fact, Information is tied for 2nd place in industries by number of varieties above 4% at 17 different Action varieties.

Figure 90 illustrates the top incidents, dominated by DDoS attacks and System Intrusions (which are driven by Ransomware). Please be sure not to forget about DDoS–while it is relatively easy to mitigate, it has certainly not gone away.

Finally, Figure 91 provides a look into something else that's easy to forget: botnets. The information industry takes the top spot in botnets for the second year running. Botnet breaches are often masked at the victim organization because they only see the malicious login, and not that the bot also stole the credentials.

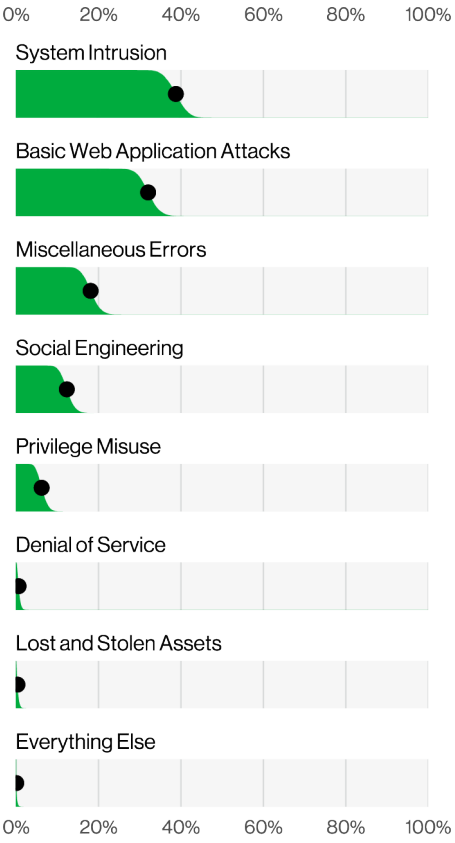

Figure 89. Patterns in Information industry breaches (n=378)

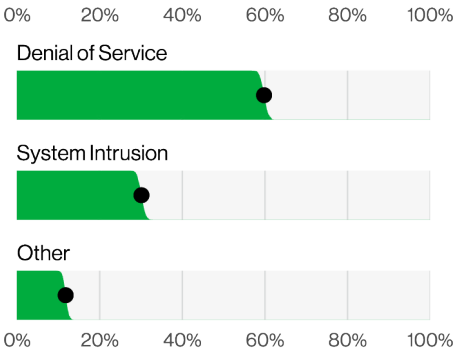

Figure 90. Top patterns in Information industry incidents (n=2,561)

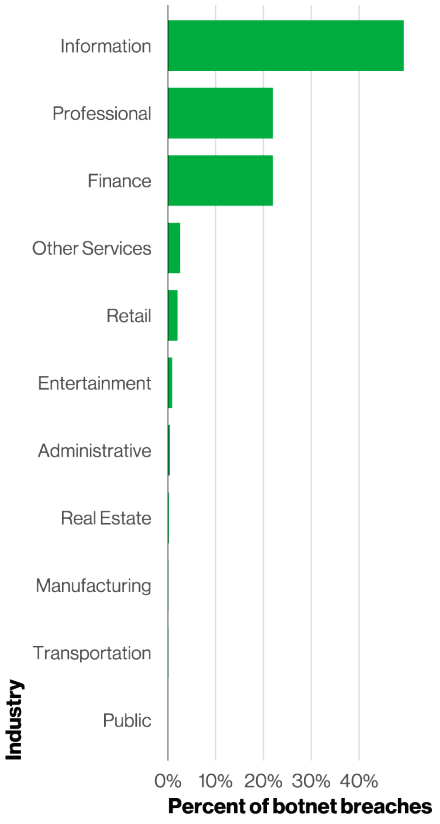

Figure 91. Evil Corp botnet breaches by industry (n=7,072)

Manufacturing NAICS 31-33

Frequency	2,337 incidents, 338 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 88% of breaches
Threat actors	External (88%), Internal (12%), Partner (1%) (breaches)
Actor motives	Financial (88%), Espionage (11%), Grudge (1%), Secondary (1%) (breaches)
Data compromised	Personal (58%), Credentials (40%), Other (36%), Internal (14%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	System intrusion and Basic Web Application Attacks continue to be among the main patterns this industry faces.

Summary

Manufacturing continues to be a lucrative target for espionage, but is also increasingly being targeted by other criminals via the use of Denial of Service attacks, credential attacks and Ransomware.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Greater
Social Engineering	Less	Less	Less
System Intrusion	Greater	Greater	Greater

Manufacturing, with its hum of machinery churning out the key components that make our modern life possible, continues to be a valued target for espionage (mostly due to recent indiscriminate supply chain attacks covered in a previous section). However, it has also become a lucrative target for financially motivated criminals looking to make a quick dollar.

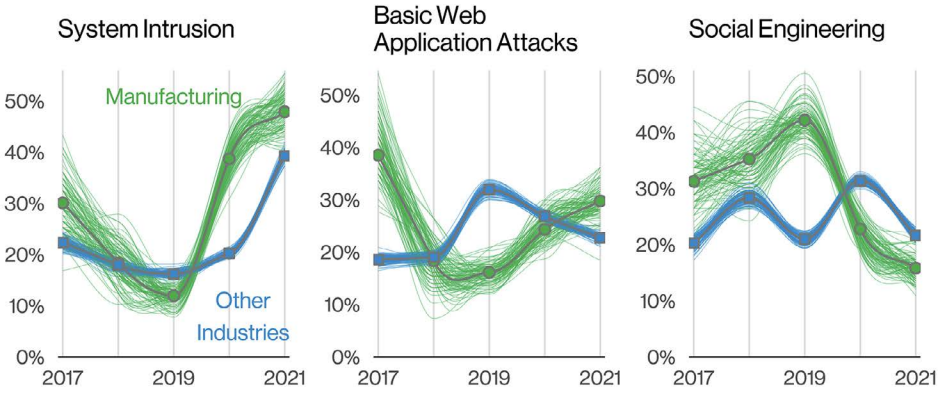

Figure 92. Top patterns over time in Manufacturing breaches

In previous reports, Manufacturing was largely targeted for their juicy schematics and secrets. For example, in 2016 over 55% of the incidents in this vertical involved Espionage (Figure 93), but that has been lower over the last few years. Or, conversely, the spies have upped their game to the point that they are no longer exposed.

DoSing against the machine

For an industry where availability equals productivity, it's interesting to see the yo-yo pattern that has been taking place with DoS attacks over the years. While DoS attacks initially reached its former peak in the 2018 report (over 40% of incidents), it's been increasing since 2019 and now accounts for approximately 70% of incidents, which puts it more in line with what we see in other industries. This rise of DoS, while unlikely to prevent those key assets from actually running the manufacturing process, is still worth keeping in mind as integration increases between the OT side of the house and the IT side.

With regard to the breaches impacting this sector, one can find the usual suspects, such as stolen credentials (39%), Ransomware (24%) and Phishing (11%) demonstrated in Figure 95. These types of breaches appear to be impacting everyone regardless of industry. Implementing safeguards, such as the ones listed in the At-a-Glance table, should be a priority for this vertical. Otherwise, you might find your organization unexpectedly seizing up due to a certain someone with an anime girl avatar.

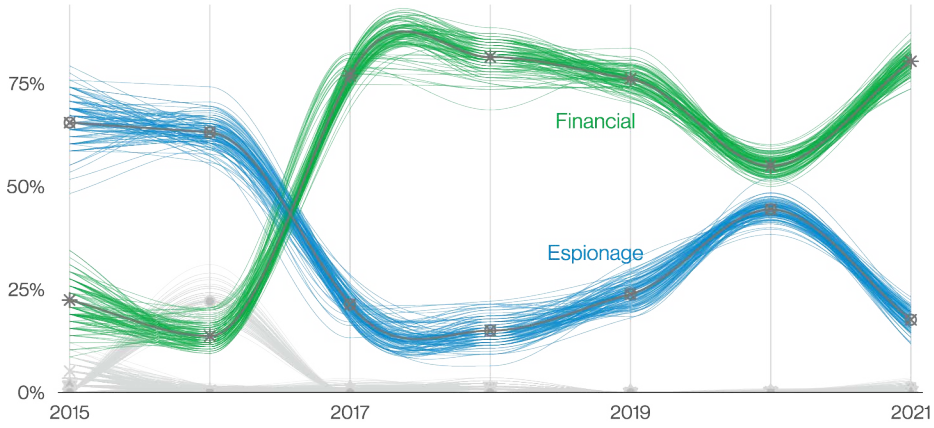

Figure 93. Motives over time in Manufacturing industry incidents

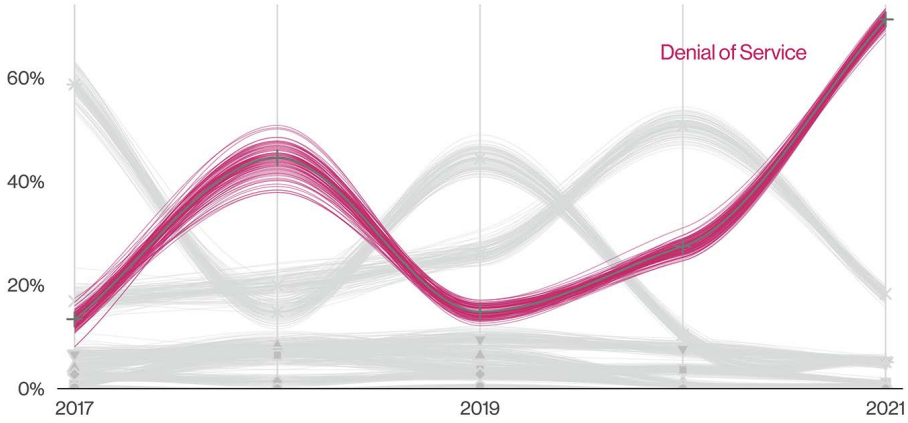

Figure 94. Patterns over time in Manufacturing industry incidents

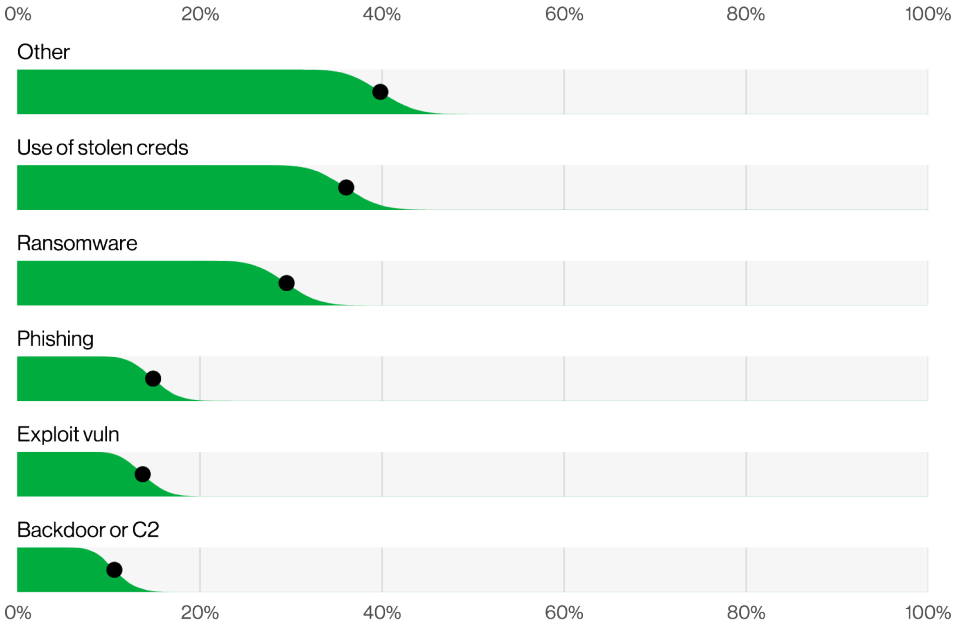

Figure 95. Top Action varieties for Manufacturing industry breaches (n=259)

Mining, Quarrying, and Oil & Gas Extraction + Utilities

NAICS 21+22

Frequency	403 incidents, 179 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 95% of breaches
Threat actors	External (96%), Internal (4%) (breaches)
Actor motives	Financial (78%), Espionage (22%) (breaches)
Data compromised	Credentials (73%), Personal (22%), Internal (9%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	This industry continues to be targeted by financially motivated actors as well as actors committing espionage.

Summary

The Mining and Utilities industry faces similar types of attacks as other industries such as those targeting credentials and leveraging Ransomware, but in addition has a high rate of social engineering attacks like Phishing.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	Less
Social Engineering	No change	No change	No change
System Intrusion	No change	No change	Less

Mining, Quarrying, and Oil & Gas Extraction + Utilities (or MQOGEU as we like to say) simply rolls off the tongue. It is an interesting "combined" industry has had a higher number of engineers. This is perhaps fitting as it seems to be under barrage from the other form of "engineers"—the Social Engineers. This industry has had a higher rate of Social Engineering breaches than their peers.

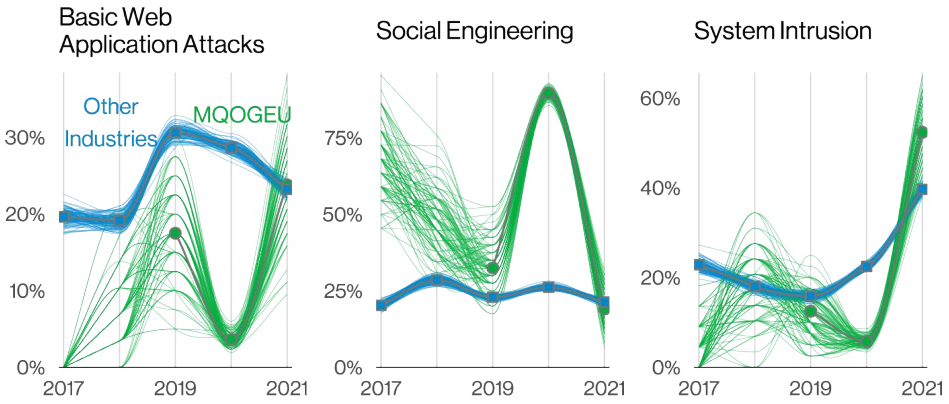

Figure 96. Top patterns over time in MQOGEU breaches

And it shows, as more than 60% of all breaches are Phishing (Figure 97), followed by stolen credentials (potentially gathered by Phishing) and Ransomware (potentially tangential to Phishing). Given the key importance of this industry to our everyday well-being, we certainly hope that those credentials aren't the only thing keeping our utilities and mining operations safe, especially since that's one of the most commonly breached data types.

Considering the high prevalence of Phishing and credential attacks, it's not too surprising to have Email servers as this industry's most commonly breached asset, followed by Web application and Desktop. Even though the infrastructure that runs these complex systems isn't traditional IT infrastructure, the company can still be exposed to the very same threats as any other organization.

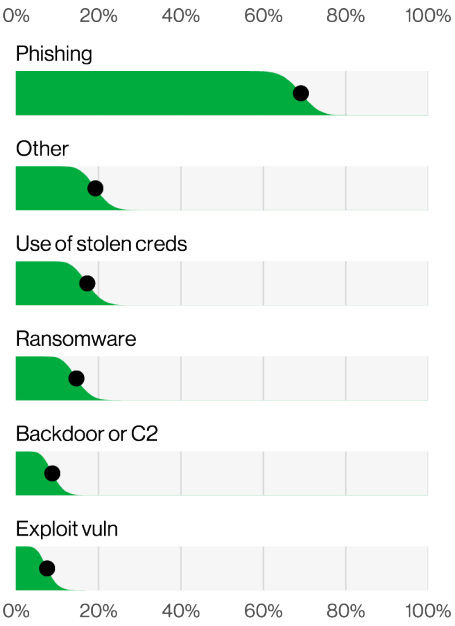

Figure 97. Top Action varieties in MQOGEU breaches (n=153)

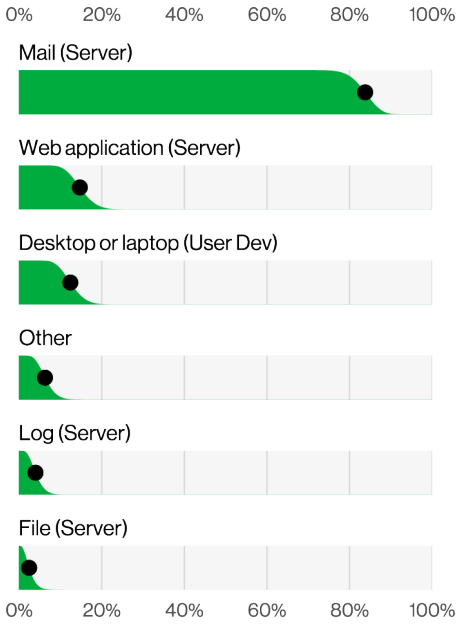

Figure 98. Top Asset varieties in MQOGEU breaches (n=130)

Professional, Scientific and Technical Services NAICS 54

Frequency	3,566 incidents, 681 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 89% of breaches
Threat actors	External (84%), Internal (17%), Multiple (1%) (breaches)
Actor motives	Financial (90%), Espionage (10%) (breaches)
Data compromised	Credentials (56%), Personal (48%), Other (26%), Internal (14%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	The top three attack patterns remain System Intrusion, Basic Web Application Attacks and Social Engineering, but they have changed order compared to last year's report.

Summary

Denial of Service attacks are a serious problem in this industry, and while they rarely result in a data breach, they can still have a significant impact. The System Intrusion attack pattern is in the first position again this year, while Social attacks are less prominent, but still in the top three.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	No change
Social Engineering	Less	Less	No change
System Intrusion	Greater	Greater	No change

Services denied

As a NAICS code with the name of Professional, Scientific and Technical Services might imply, this sector relies on their internet presence to provide their highly skilled offerings to their customers. This means that when they are hit with a DoS attack, particularly the higher volume distributed varieties, they definitely feel the impact. This past year has been a hard one for this sector, with the DoS attacks accounting for almost half of the incidents recorded. And even though this type of attack rarely leads to a reportable data breach, it can still do significant damage to the victim.

The devil you know

Moving to breaches, the System Intrusion pattern remained at the top of our pyramid, while Basic Web Application Attacks and Social Engineering switched places. So, the same players remain on the field, they are simply playing different positions.

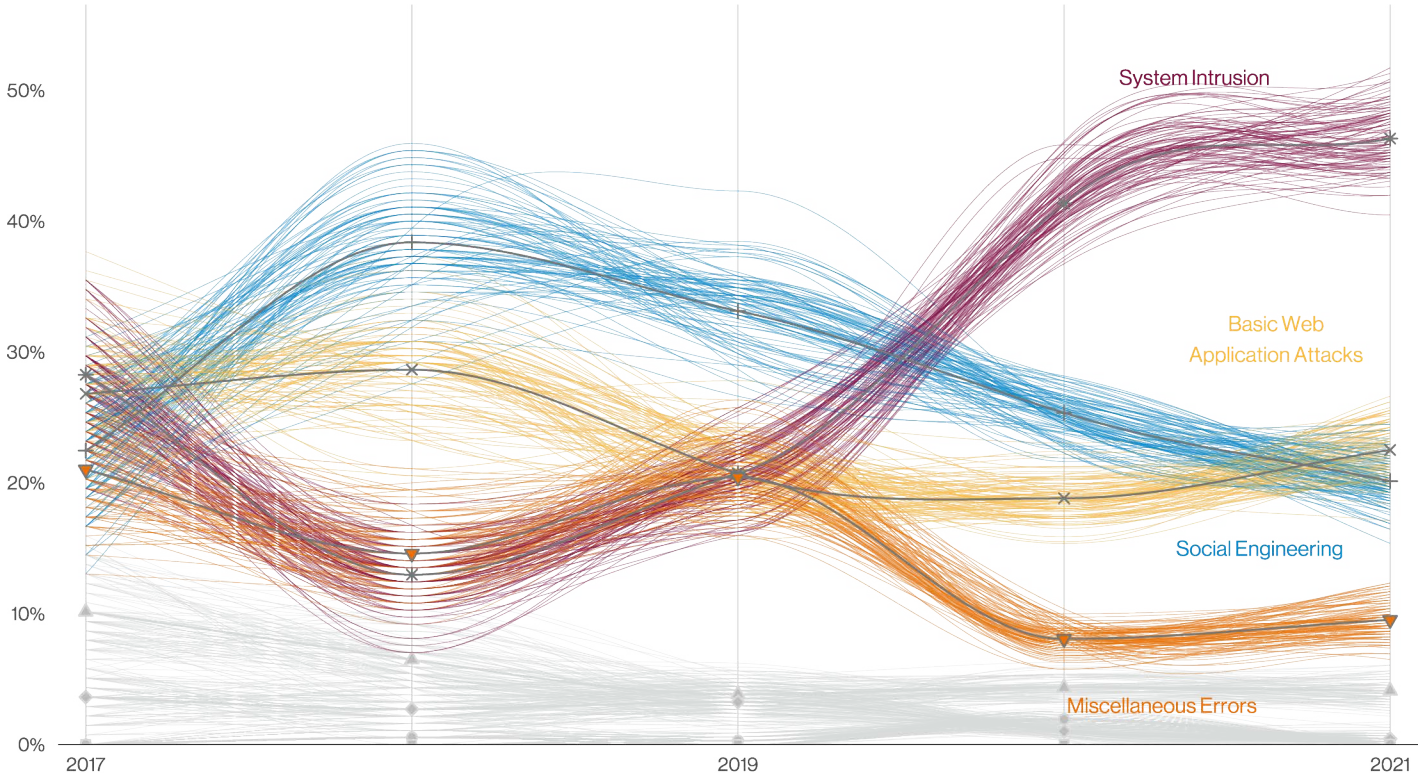

Figure 99. Patterns over time in Professional, Scientific and Technical Services breaches

The perpetrators of these top three attack patterns tend to be External. The Internal actor breaches were down this year by comparison to last year's report. Surprisingly we saw a small uptick in the multiple actor breaches in this sector this year. These are when an external actor recruits an internal or partner actor to help them out with the breach activities. Sometimes they are paid for their troubles, and sometimes it is a more subtle form of influence by an acquaintance or significant other exerting pressure on the person with the access to data. Either way, the result is a breach that can be more difficult to detect, since it is someone on the inside facilitating the access under the guise of conducting their regular duties.

Days gone by

Looking back over the years in this sector, the Miscellaneous Errors pattern was in the top three. However, as Figure 99 shows, in 2019, the System Intrusion pattern began its meteoric rise to the top, eventually far surpassing Errors. This sector mirrors the overall dataset in terms of the top attack patterns. The top three here are the top three patterns in the full dataset, so clearly, these patterns are holding sway in a number of business categories.

Public Administration NAICS 92

Frequency	2,792 incidents, 537 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 81% of breaches
Threat actors	External (78%), Internal (22%) (breaches)
Actor motives	Financial (80%), Espionage (18%), Ideology (1%), Grudge (1%) (breaches)
Data compromised	Personal (46%), Credentials (34%), Other (28%), Internal (28%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	Miscellaneous Errors remain in the top three patterns in the same place as last year.

Summary

The System Intrusion pattern is the newest big dog to arrive on the scene in this sector. Employees continue to be a cause of breaches in this vertical, although Internal actors are seven times more likely to make a mistake than to commit a malicious act that causes a breach.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
Miscellaneous Errors	No change	Less	Less
System Intrusion	Greater	Greater	Greater

Here and now

The System Intrusion pattern has drop-kicked the Social Engineering pattern right out of the "top three" club. This was quite the coup, considering the Social Engineering pattern was in the top spot last year. In part, this may be attributed to some prominent and far-reaching supply chain breaches that came to light last year.

As the Social Engineering pattern fell, the Basic Web Application Attacks stepped in to fill the vacuum. Miscellaneous Errors remained in the middle spot, with the trio of Misconfiguration, Misdelivery and Loss nearly tied for what caused the most error-based breaches in this sector.

The occurrence of errors in this industry accounts for the prevalence of breaches caused by the Internal actor. While there was a smattering of Misuse breaches in this sector, Internal actors are about seven times more likely to make a mistake that causes a breach than they are to do something malicious.

We have said before how popular Credentials are as a data type to be raided. However, this year's data showed a drop from 2021's report, when it was 80% in this industry. Personal was only 18% last year, but has now catapulted into the top spot.

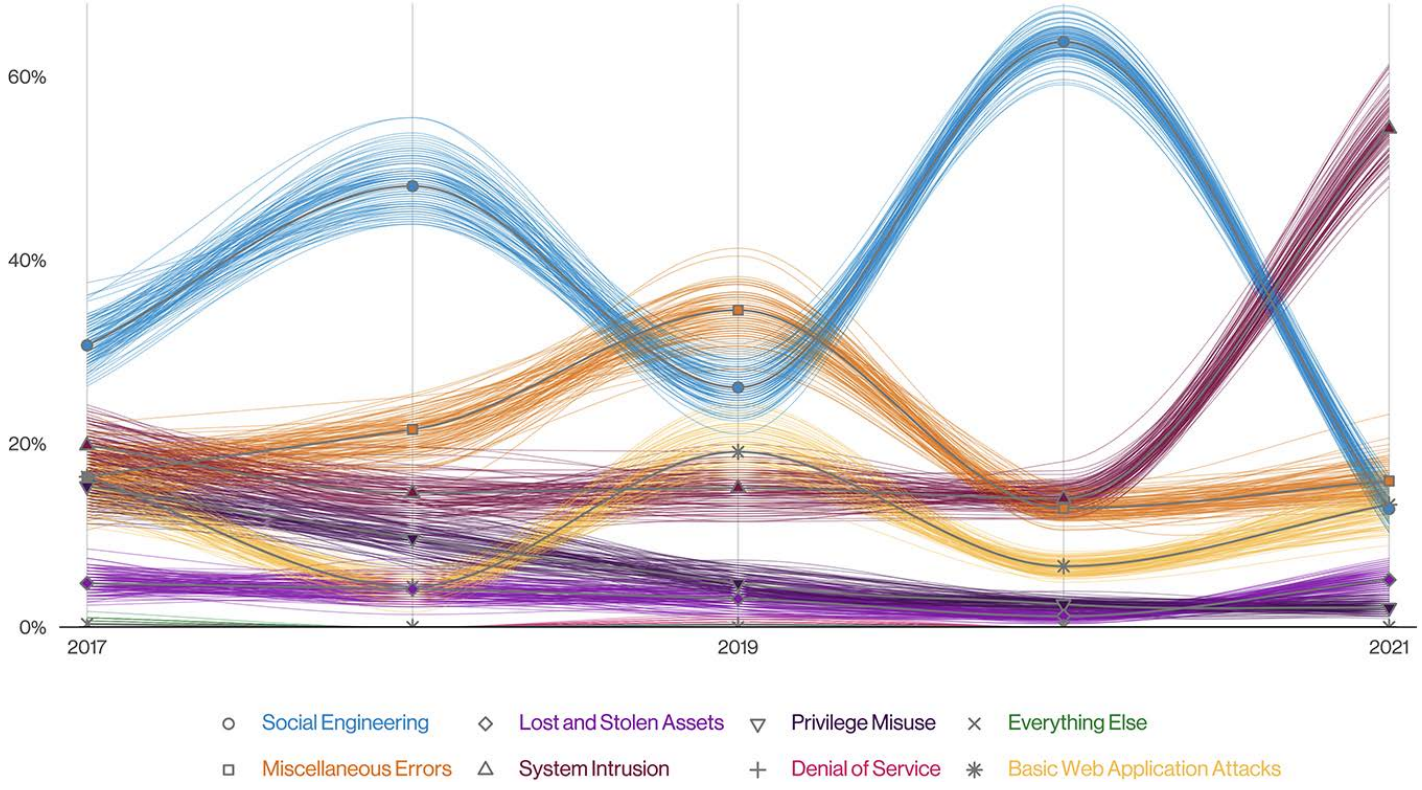

Figure 100. Patterns over time in Public Administration breaches

Step into my raggedy DeLorean

In honor of our 15-year anniversary, we wanted to take a look back in time at what has changed in this sector. Just three years ago, the top motive was Espionage, at 66% of breaches. Five years ago, it was 64%, which illustrates that it has been a persistent challenge for Government entities. This makes sense, when you consider that regardless of which Government entity we are talking about, someone wants to know what they're up to. Speaking of malicious—we found that the Espionage motive is up from 4% from last year to 18% this year. Internal breaches also increased from last year, and we have the motive of Grudge popping up in our list for a change.

Figure 101 illustrates the change in the Espionage-motivated actors in this industry since 2017. As you can see, when the Espionage motive fell, the Financial-motivated attacks rose. It appears that the Public Administration sector has joined the rest of us in being targeted by criminals looking to make a buck. Welcome to the party, pal![27]

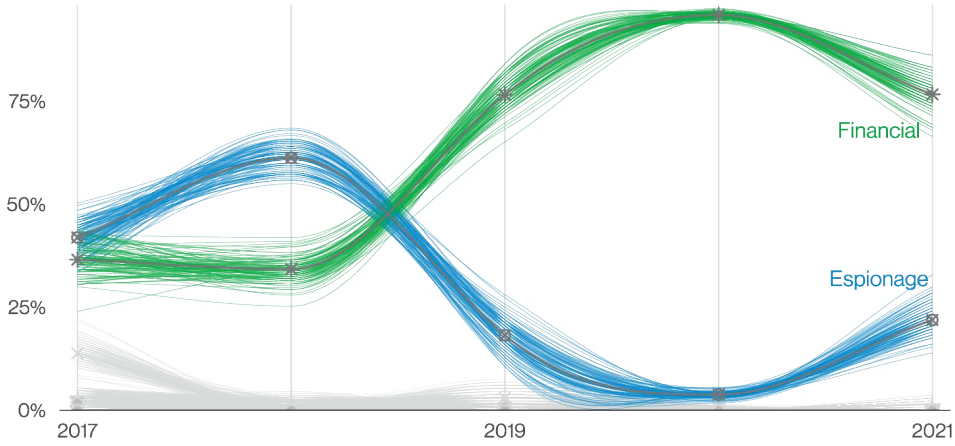

Figure 101. Actor motives over time in Public Administration breaches

27 Admit it, you read this in John McClane's voice.

Retail NAICS 44-45

Frequency	629 incidents, 241 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 84% of breaches
Threat actors	External (87%), Internal (13%) (breaches)
Actor motives	Financial (98%), Espionage (2%) (breaches)
Data compromised	Credentials (45%), Personal (27%), Other (25%), Payment (24%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	These organizations continue to be impacted by a variety of threat actors that leverage a range of tactics such as deploying malware to capture credit cards being processed by webforms and more common tactics like phishing.

Summary

The Retail industry is experiencing the same types of attacks they suffered last year: Use of stolen credentials, Phishing and Ransomware.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Less	Less
Social Engineering	No change	Greater	Greater
System Intrusion	Greater	No change	Greater

Our society, indeed the entire globe, has seen an astounding amount of change over the last couple of years. The Retail industry, on the other hand, has not, at least when it comes to breaches. As tempting as it was to simply cut and paste our findings for this industry from last year's report, we bravely refrained from doing so. Nevertheless, while the needle has not moved very much from when we last looked at it, there are a few noteworthy findings.

Social attacks, roughly split between Phishing (53%) and Pretexting (47%), have been on the rise over the last few years in the Retail industry: 7% in 2016, 13% in 2018, 29% this year. This accounts for Social Engineering's position in the top three patterns. Therefore, as one might expect, Credentials are the top data type compromised in this vertical. In many cases those Credentials are later utilized to hack into servers and load ransomware (47%). Then the criminals sit back and wait for a big payday.

One interesting finding this year is that the Malware enumeration of "Capture app data" in the Retail industry is 7 times higher than the other industries. This goes some way to explain why the System Intrusion pattern is ranked at first place in this industry. The "Capture app data" functionality is one that we commonly see in Magecart-type attacks, in which the attacker will typically exploit a vulnerability, use stolen credentials to gain access to an e-commerce server and then just chill there and take a little sumpin' sumpin' for themselves, almost always payment card data.

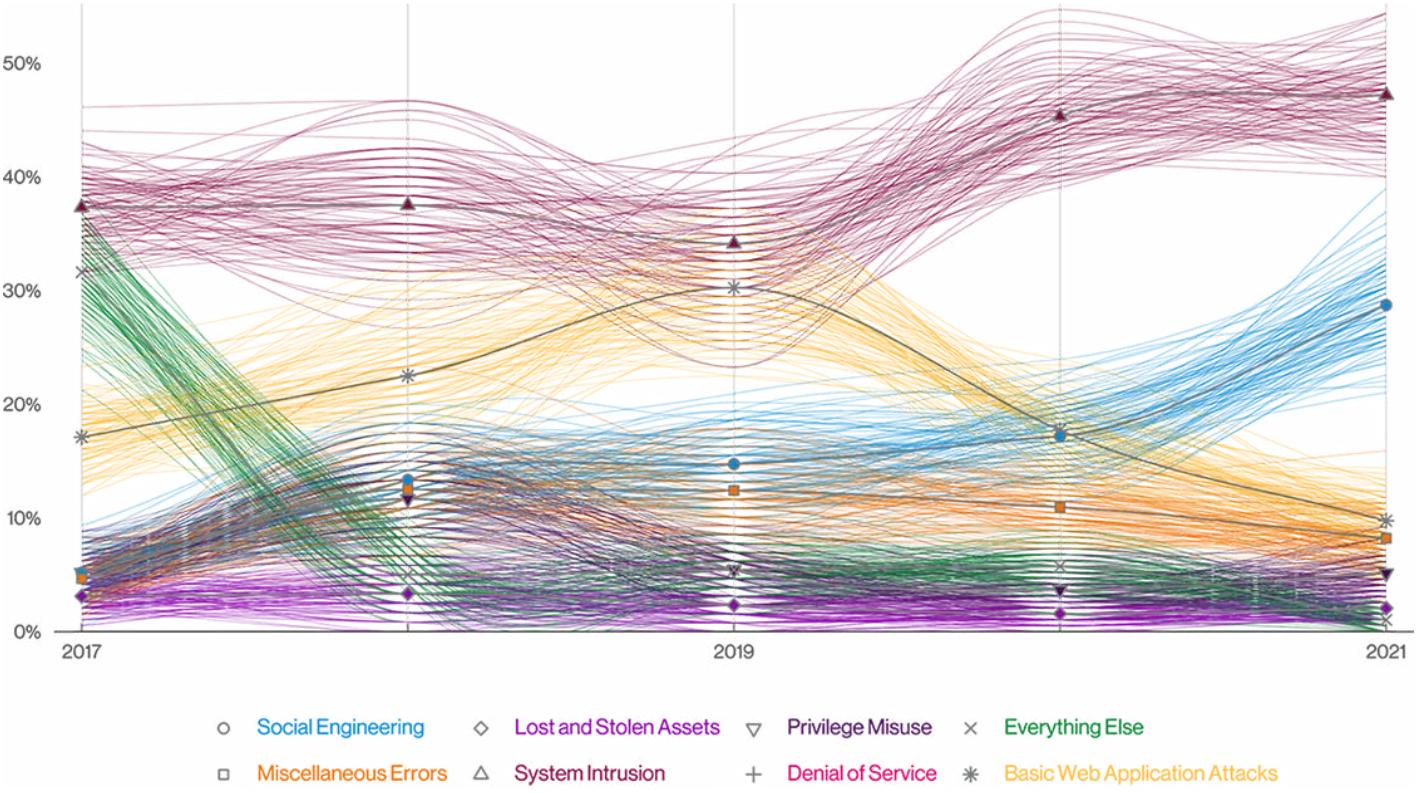

Figure 102. Patterns over time in Retail industry breaches

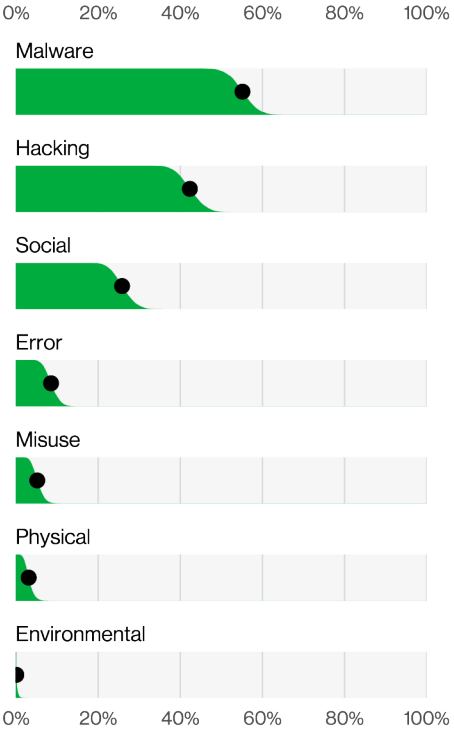

Figure 103. Actions in Retail industry breaches (n=241)

Finally, when a company in the Retail industry learns that they have become a victim, it's via fraud detection mechanisms (e.g., Common Point of Purchase [CPP] or law enforcement) more than any other industry. This is perhaps a rather intuitive finding given the fact that Retail is responsible for so many transactions, but it is noteworthy nonetheless.

Very Small Business Cybercrime Protection Sheet

Frequency	832 incidents, 130 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Privilege Misuse represent 98% of breaches
Threat actors	External (69%), Internal (34%), Multiple (3%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Credentials (93%), Internal (4%), Bank (2%), Personal (2%) (breaches)

When cybercrime makes the news, it is typically because a large organization has fallen victim to an attack. However, contrary to what many may think, very small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so. Threat actors have the "we'll take anything we can get" philosophy when it comes to cybercrime. These incidents can and have put small companies out of business. Therefore, it is crucial that even very small businesses (10 employees or less) should take precautions to avoid becoming a target. Large organizations have large resources, which means they can afford Information Security professionals and cutting-edge technology to defend themselves. Very small businesses on the other hand have very limited resources and cannot rely on a trained staff. That is why we wrote this section.

If you own or manage a very small business, we offer the following recommendations or best practices. We suggest you print out or tear out this section and refer to it when a concern appears.

What are the most common threats facing my business?

The number one action type in our dataset for very small businesses are ransomware attacks. Ransomware is a type of malicious software that encrypts your data so that you cannot view or utilize it, and once the ransomware is triggered the threat actor demands a (frequently large) payment to unencrypt it. This is where having those offline[28] backups come in handy.

The second most common is the Use of stolen credentials. Attackers can get your credentials (username and password) via many different methods. Brute force attacks (where attackers use automation to try numerous combinations of letters, symbols and numbers to guess your credentials), various types of malware (thus the value of having an up-to-date Antivirus), reused passwords from another site that has been hacked and last but not least, social attacks such as Phishing and Pretexting.[29]

You may have heard the term "Business Email Compromise" in news articles. They typically involve Phishing and/or Pretexting, and can be quite convincing, (such as an invoice that looks like it comes from a known supplier but has a different payment account, or an email from a business partner saying they're in a pinch and need a quick payment made on their behalf). While most come in through email, criminals have also employed the telephone to convince their target that this is a legitimate request. The criminal element often run their enterprise just like a legitimate business and may even take advantage of criminal call centers (yes, these exist) to help lend credence to their ploy.

Phishing is a type of social attack

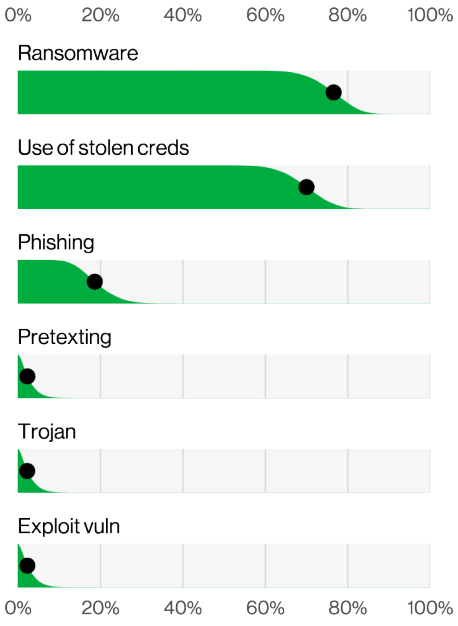

Figure 104. Action varieties in 1 to 10 employee organization breaches (n=61)

28 If you're unsure what "offline" means here, see "What to do to avoid becoming a target" below.
29 If you're not familiar with "phishing" or "pretexting," it's okay. Keep reading for the definitions.

(usually via email) in which the attacker tries to fool you into doing something you should not, such as providing them with your user name and password or clicking on a malicious link. Examples include "click here to reset your password" or download an invoice, view the pdf attachment, verify your bank account number, etc. These attacks can be extremely realistic and are often very hard to identify.

Pretexting is the human equivalent of Phishing. Typically, the threat actor attempts to create a dialog with the victim by impersonating a business partner, a bank employee, or a superior in your own organization in order to gain access to login information. The end game for Pretexting is usually the automated transfer of funds from your organization to the criminal's bank account.

How do I know I have become a victim?

Watch for anything strange or out of the ordinary. For example, you might see unexpected charges on your bank statement or phone bill. Keep an eye out for transactions on your credit card that you don't recognize. You may receive comments from friends about emailed requests for them to buy a gift card. You may receive phone calls asking for your password or credit card number, or a request to change the account number or how you pay a regular vendor or client. All of these things are warning signs that something malicious might be happening. Think of your computer like a car–if it suddenly won't start, runs slower or makes a weird noise, it's time to have an expert take a look. Finally, with threats such as ransomware the threat actor will actually alert you that your data has been encrypted.

What to do to avoid becoming a target

1. Use two-factor authentication[30]
2. Do not reuse or share passwords[31]
3. Use a password keeper/generator app
4. Be sure to change the default credentials of the Point of Sale (PoS) controller or other hardware/software
5. Ensure that you install software updates promptly so that vulnerabilities can be patched
6. Work with your vendors to be sure that you are as secure as you can be, and that they are following these same basic guidelines
7. Keep a consistent schedule with regard to backups and be sure to maintain offline backups—meaning that they are not on a device connected to a computer
8. Ensure that the built-in firewall is switched on for user devices such as laptops and desktops ("on" may not be the default)
9. Use antivirus software, for all your devices. Smart phones, tablets and credit card swipers are just as important as laptops and computers. It won't catch everything, but it will help
10. Do not click on anything in an unsolicited email or text message
11. Set up an out of band method for verifying unusual requests for data or payments
12. Make sure the computer used for financial transactions is not used for other purposes such as social media or email
13. Use email services that incorporate phishing and pretexting defenses and use a web browser that warns you when a website may be spoofed

Who do I contact if I learn I have been a victim of cybercrime?

- A large range of resources for many different situations is available through https://fightcybercrime.org/. This website provides information on where to go and what to do in the event of a cyber incident
- Scam Spotter provides simple, easy-to-understand information about how to recognize common scams: https://scamspotter.org/
- If you are in the United States, your state's Attorney General's office website may have resources for you as well

Familiarize yourself with these resources, and draw up a plan for what steps you will take if you find your organization has become a victim. Plan this ahead of time instead of waiting until your company's "hair" is on fire. Even if it is just a document that contains the contact information for all of your vendors and your bank's fraud department, it is a place to start. Print it off and post it somewhere you can access it easily. Don't just keep it on your computer—it might be unavailable as part of the attack.

Some planning on your part, along with a bit of educating the people most likely to encounter these kinds of attacks, can go a long way in helping to make your small company safer.

30 This adds an additional layer to just the username and password combination. It may be a code that is texted to your registered cell phone, the use of an authenticator app like Google or Microsoft Authenticator, or the use of a little device that you plug into a USB drive when prompted. If your vendors do not offer two-factor authentication (also called multi-factor authentication or MFA), start lobbying for them to accommodate it.

31 Not between people and not between applications or websites. A password keeper makes this easier.