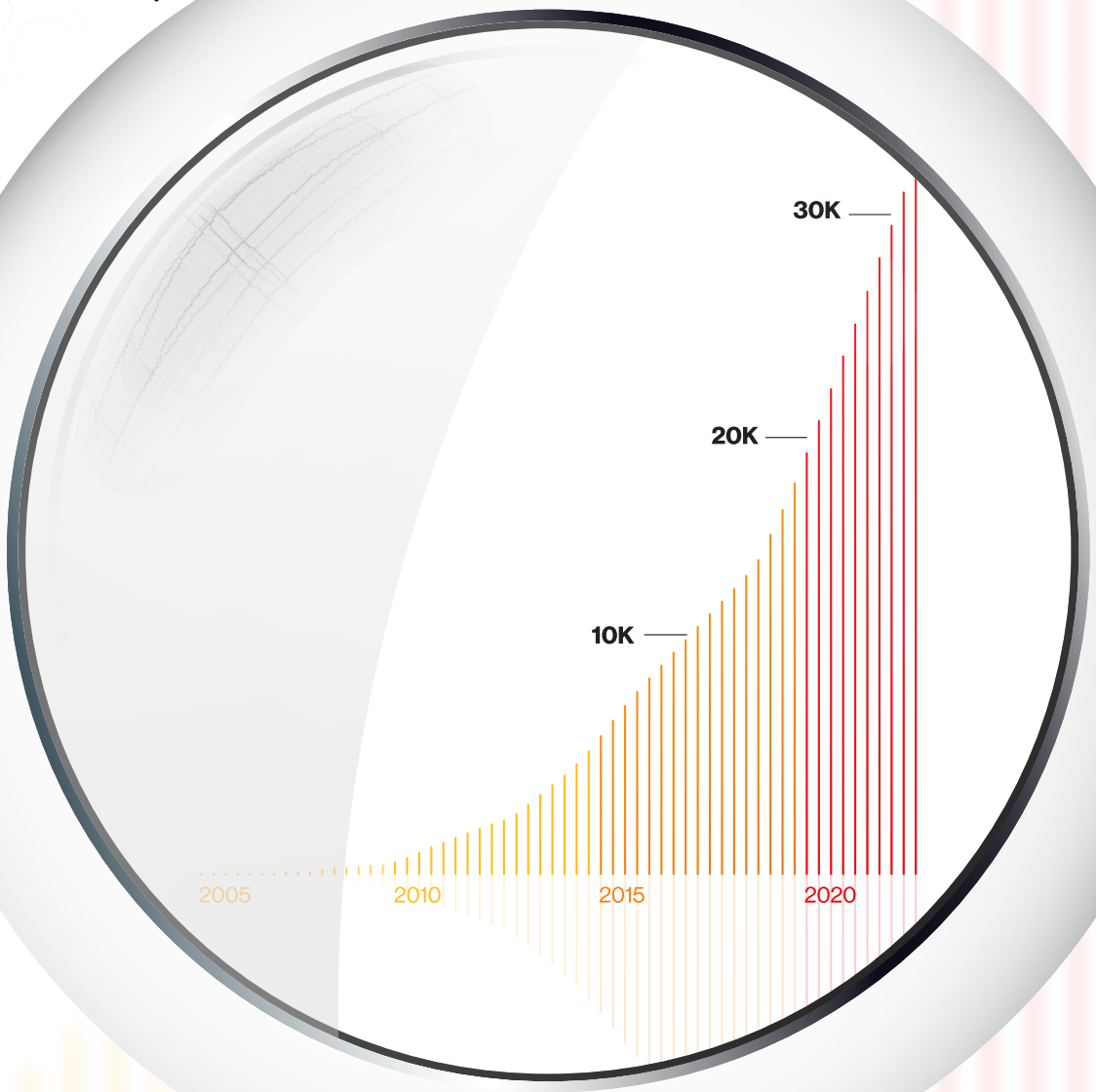
DBIR

2023 Data Breach Investigations Report

Small and Medium Business Snapshot



verizon

About the cover

The magnifier on the cover is intended to visually convey the effort the team made to refocus our energy and resources more on our core breach dataset. The graph that is magnified is simply a cumulative count of the number of breaches in our dataset as the years have gone by since our first report. Long-time readers may notice the Vocabulary for Event Recording and Incident Sharing (VERIS) Framework trademark honeycombs, which are meant to convey the 4As (Actor, Action, Asset, Attribute) and their various enumerations.

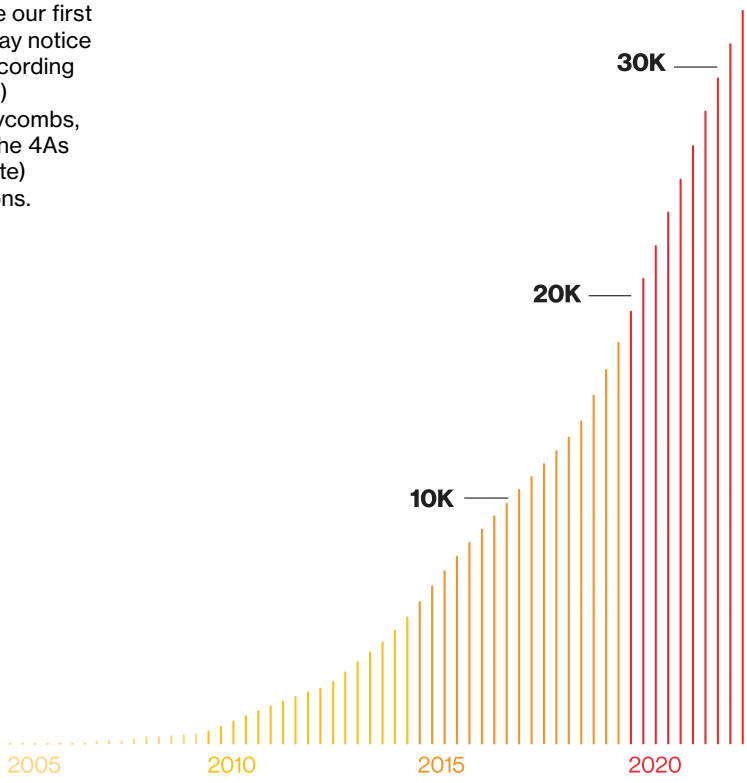


Table of contents

Welcome

Hello, and welcome to the 16th annual installment of the Verizon Data Breach Investigations Report (DBIR) Small and Medium Business Snapshot.

The DBIR aims to provide security professionals with an in-depth analysis of data-driven, real-world instances of cybercrime and how cyberattacks play out across organizations of different sizes as well as from different verticals and disparate geographic locations. We hope that by doing so, we can provide you with insight into what particular threats your organization is most likely to face and thereby help prepare you to handle them in the best possible manner.

As in past years, we will examine what our data has to tell us about threat actors and the tools they employ against enterprises. This year, we looked at 16,312 security incidents, of which 5,199 were confirmed breaches.

This data represents actual, real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC), now celebrating its 20th year, or provided to us by one of our global contributors without whose generous help this document could not be produced. We hope you can use this report and the information it contains to increase your awareness of the most common tactics used against organizations at large and your specific industry. It offers strategies to help protect your company and its assets. Read the full report for a more detailed view of the threats you may face today at verizon.com/dbir.

16,312
security incidents investigated

5,199
confirmed breaches

Summary of findings

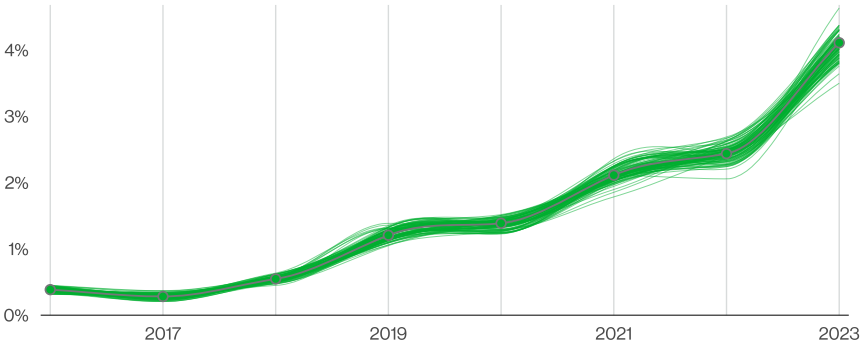


Figure 1. Pretexting incidents over time

Business Email Compromise is a key issue.

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 1, and now represent more than 50% of incidents within the Social Engineering pattern.

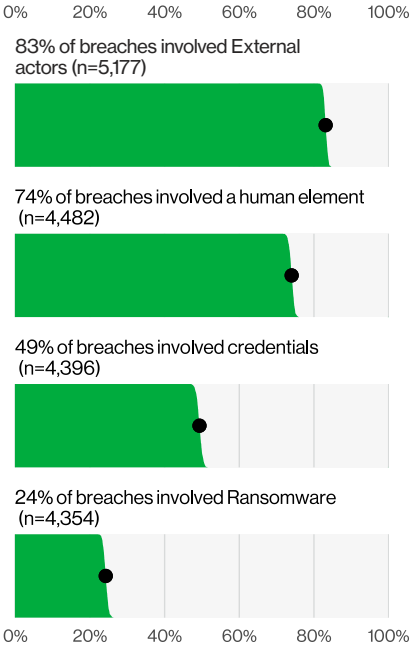


Figure 2. Select key enumerations

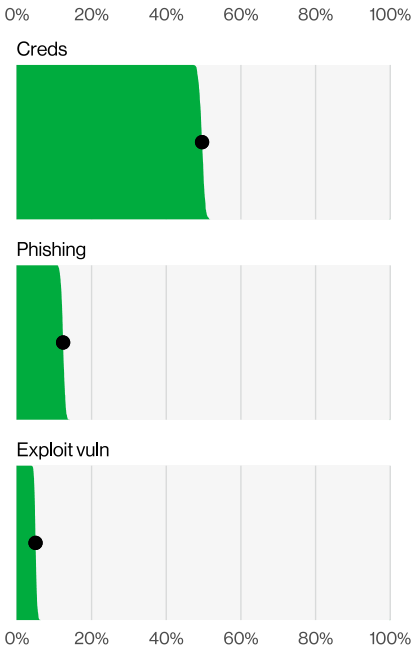


Figure 3. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

The human element risk cannot be understated.

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

Looking for access on multiple fronts.

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

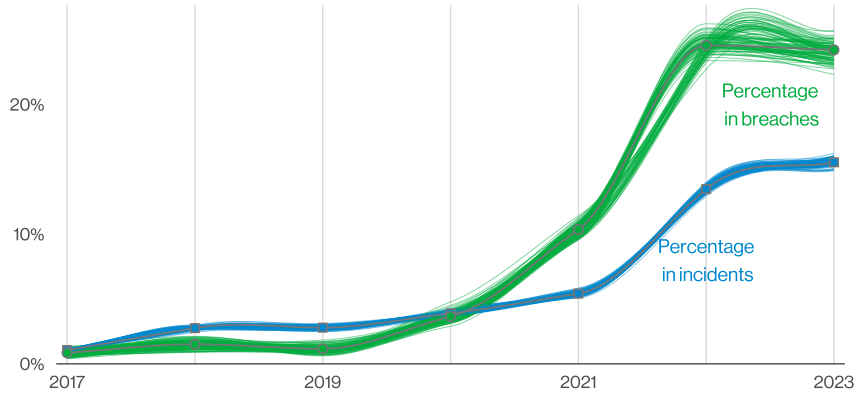


Figure 4. Ransomware action variety over time

Ransomware remains a top action type.

Ransomware continues its reign as one of the top action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

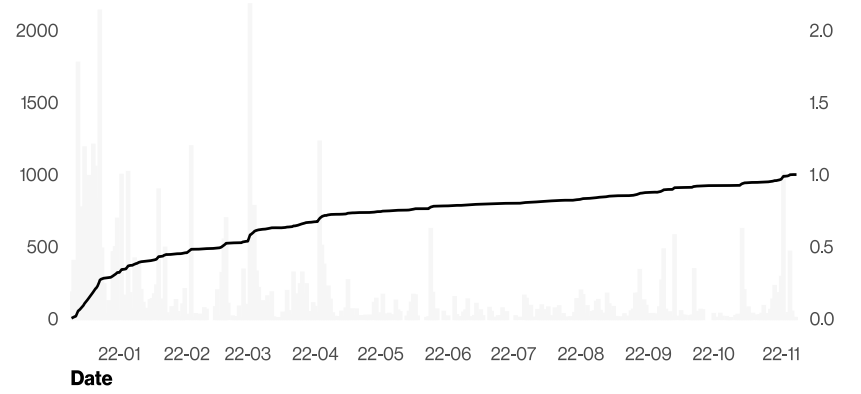


Figure 5. Percentage of Log4j scanning for 2022

The Log4j scanning concentrated near release.

More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

Figure 6. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

Log4j was so top-of-mind in our data contributors' incident response that 90% of incidents with Exploit vuln as an action had "Log4j," or "CVE-2021-44228" in the comments section. However, only 20.6% of the incidents had comments.

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. Last year, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to eight—the seven you see in this report and the Everything Else "pattern," which is a catch-all for incidents that don't fit within the orderly confines of the other patterns.

These patterns are based on an elegant machine-learning clustering process, equipped to better capture complex interaction rules, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

Here are our key findings for each pattern:

System Intrusion	These are complex attacks that leverage malware and/or hacking to achieve the objectives. Frequently included in this pattern is the deployment of ransomware.	80% of System Intrusion incidents involved Ransomware as attackers continue to leverage a bevy of different techniques to compromise an organization and monetize their access. • 91% of industries have Ransomware as one of their top varieties of incidents. • 32% of Log4j vulnerability scanning occurred within 30 days of the vulnerability's release. • 97% of breaches were Financially motivated, and 3% were motivated by Espionage. • While only 7% of Ransomware incidents reported losses to the FBI Internet Crime Complaint Center (IC3), the median loss more than doubled from last year to $26,000, with 95% of incidents ranging between $1 and $2.25 million.
Social Engineering	This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.	Social Engineering incidents have increased from the previous year largely due to the use of Pretexting, which is commonly used in BEC, almost doubling since last year. • Based on IC3 data, the median amount stolen from these attacks has increased over the last couple of years to $50,000. • Social Engineering accounts for 17% of Breaches and 10% of Incidents.

Basic Web Application Attacks	These attacks are against a web application (as the name implies), and after the initial compromise, they typically do not have a large number of additional Actions. This is the "get in, get the data and get out" pattern.	While representing approximately one-fourth of our dataset, Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against credentials and then leveraging those stolen credentials to access a variety of resources. • 86% of Basic Web Application Attacks breaches involve the Use of stolen credentials. • 10% of breaches in this pattern involve the Exploitation of a vulnerability.
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset fall into this pattern. This does not include lost devices, which are grouped with theft in the Lost and Stolen Assets pattern.	Error-related breaches are down to 9% as opposed to 13% last year. However, this could be due to sample size (715 error incidents and 708 with confirmed data disclosure in last year's data as opposed to 602 incidents, with 513 confirmed breaches this year). • Data compromised included Personal (89%), Medical (19%), Other (10%) and Bank (10%). • Misdelivery (sending something to the wrong recipient) accounts for 43% of breach-related errors. • Publishing errors (showing something to the wrong audience) is in second place at 23%. • Misconfiguration comes in third and accounts for 21% of error-related breaches. • The majority of errors that lead to breaches are committed by Developers and System admins.
Denial of Service	These attacks are intended to compromise the availability of networks and systems, which includes both network and application layer attacks.	The median size of attacks grew 57% from 1.4 gigabits per second (Gbps) last year to 2.2 Gbps this year, and the top size of attacks, the 97.5 percentile, grew 25% from 99 Gbps to 124 Gbps. • A point of attention that some of our partners brought to us was the growth of distributed DNS Water Torture attacks in, you guessed it, shared DNS infrastructure.
Lost and Stolen Assets	Any incident where an information asset went missing, whether through misplacement or malice, is grouped into this pattern.	The loss and theft of mobile phones continues to be an issue across the board. While less data tends to be on these devices, the same cannot be said of laptops, While less data tends to be on these devices, the same cannot be said of laptops, the loss and theft of which increased last year.
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges are grouped here.	We are increasingly seeing Privilege Misuse breaches paired with Fraudulent transactions, more so this year than in the past several.

Table 1. Incident Classification Patterns key findings

Insights for small and medium business

"Let's do some word problems!"—said no one ever (except math teachers)

In certain prior reports, we have compared and contrasted small and medium businesses (SMBs) against large organizations to determine whether the attack surface differed significantly between them. Increasingly, both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked.

The tables on the right illustrate the fact that SMBs and large organizations have increasingly become similar to each other. This phenomenon began several years ago, and by now there is so little difference based on organizational size that we were hard-pressed to make any distinctions whatsoever. Therefore, this year we decided to look at these a bit differently by looking at the implementation of security controls for various size SMBs (smaller, midsize and larger) and how they may overlap or differ.

In past reports we have discussed the research we conduct with regard to controls—in particular, the work we have done with MITRE to map VERIS to ATT&CK. This year, we would like to take this research a bit more into the real world and apply it to how you would use these mappings with the appropriate Center for Internet Security (CIS) Implementation Group protective controls.

Small businesses (less than 1,000 employees)	
Frequency	699 incidents, 381 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

Table 2. At a glance for SMBs

Large businesses (more than 1,000 employees)	
Frequency	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Table 3. At a glance for large organizations

It's not easy being small.

Let's assume you're a startup—a tiny company in its infancy. You have very, very limited resources for implementing security controls of any kind. Your IT person is also your security person is also your Jack- (or Jill-) of-all-trades who wears many hats and never sleeps.

The first step is to see which controls are recommended for your level of security maturity and resources. But where to begin? We like the CIS Critical Security Controls Navigator as a good starting point.[1] It breaks down each of the CIS Controls into small, easy-to-consume chunks and then maps them to various security standards that an organization may want to comply with as their adopted standard. You will see that they are broken into three Implementation Groups, and each one is geared to the organization's maturity level. Since we're at the beginning here, we will start with Implementation Group 1 (IG1). While these are all good controls and should be on the road map, let's take a more threat-centric approach in our scenario.

You can see in in Tables 2 and 3 that regardless of an organization's size, they are most commonly going to face the System Intrusion pattern. In last year's report, we mapped the Controls to the pattern and showed which were most commonly going to help you in an attack. The result in IG1 shows Controls 14 (89%), 11 (80%) and then 5 (67%).[2]

When you drill further into the Sub-Controls, more granularity should guide you in your quest for maturing your organization's security posture. Each organization will need to customize and prioritize according to its own risk profile and tolerance, but it is at least a place to begin. Once the most likely suspects are accounted for, move onto the next mostly likely attack pattern you may be facing and determine how to handle that. Using data-driven information on your most probable risk areas is a defensible strategy toward prioritizing controls with few resources. Hopefully after some progress is made, your Jack-/Jill-of-all-trades can go back to sleeping at night.

Control	Description
14	**Security Awareness and Skills Training** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
11	**Data Recovery** Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a preincident and trusted state.
5	**Access Control Management** Use processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator and service accounts for enterprise assets and software.

Table 4. CIS IG1 Controls most commonly encountered by SMBs

1 https://www.cisecurity.org/controls/cis-controls-navigator/
2 2022 DBIR, Appendix B: VERIS and Standards, p. 96

Midsize is the right size.

You've been at this a while. You're not tiny, but you're not quite at the enterprise level just yet. You have been working diligently at maturing your processes in both IT operations and in information security. You have put in place the Controls in IG1 and are now eyeing IG2 to take your company to the next level of protection.

With that in mind, let's take a look at the IG2 controls that cover the Social Engineering pattern, which is the second largest threat for SMBs. The first two controls are the same main categories as they were for System Intrusion, Control 5 (100%) and Control 14 (100%). However, the third control is different for this pattern:

- **Control 17 – Incident Response Management**
  Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.

An Incident Response Management plan is key to all areas of security but perhaps especially so when it comes to Social Engineering attacks for a few reasons. Many of these attacks, such as pretexting, tend to escalate quickly and can have a high impact. Perhaps just as importantly, employees need to feel secure in the knowledge that they have a place they can report these incidents to when they occur because the sooner they report them, the more quickly you can address them.

"You get a resource! You get a resource! Everybody gets a resource!"

Now let's pivot to look at the larger organizations in the SMB area. To clarify, we are still writing with regard to SMBs, we simply mean the larger companies that still fall into that category (<1,000 employees). When your company reaches this point, there are more resources available to throw at problems, whether in the form of more people, more technology options or just plain more cash, and bringing those resources to bear can yield substantial benefits. At this, level you may have tackled IG1 and IG2 and are ready for IG3 Controls.

These Controls mature along with your organization. Therefore, let us examine the IG3 Controls with regard to the third most common pattern for SMB: Basic Web Application Attacks. The first, Control 17 (100%), we talked about in the previous section, but Controls 16 (100%) and 18 (100%) we have not yet discussed.

- **Control 16 – Application Software Security**
  Manage the security life cycle of in-house developed, hosted or acquired software to prevent, detect and remediate security weaknesses before they can impact the enterprise.

- **Control 18 – Penetration Testing**
  Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes and technology), and simulating the objectives and actions of an attacker.

Control 16 is certainly timely, considering the SolarWinds case from last year's report and the Log4j impact discussed in this year's report, so we should have no problem seeing the relevance of this Control. Sub-Controls 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities, 16.4: Establish and Manage an Inventory of Third-Party Software Components, and 16.5: Use Up-to-Date and Trusted Third-Party Software Components would have gone a long way to defending against both of those cases.

Once an entity has reached the large organization status, Control 18 also comes into play. Establishing penetration testing capabilities and incorporating their findings into the security processes can only improve the information security posture of a large organization. This is basically real-world testing of your controls to make sure they are performing how you expect them to. Like backups, only controls that have been tested and verified should be trusted.

Now that you've already looked at the Controls and prioritized them, you know what you're most likely to be hit with and you're working your way through to the end—your ducks are almost all in a row. You have balanced preventive and detective capabilities and are on your way to being able to not only detect when something bad has happened but also respond quickly and appropriately. You have moved from the basics of putting your plan together to implementing a road map.

A few final things to consider at this point: Are you looking at aligning with a particular compliance framework? Do you track metrics around security in your environment? Do your efforts result in ongoing improvements to your security posture, or do they just provide a point-in-time snapshot that says, "I was good at this moment, but then things changed"? There is quite a bit you can do when you use good information about what is happening in your organization to steer your security strategy.

From the Center for Internet Security:

Report after report, and study after study, shows that many attacks are successful because network owners did not know their enterprise assets, the software they had running and where their critical data was. Knowing your environment is foundational to any cybersecurity program, so they encompass the first three controls of the CIS Critical Security Controls (Controls). After all, you can't protect what you don't know you have.

After understanding your environment, you can prioritize where to apply and which controls to implement across your enterprise. At CIS we know that this will take time and resources, which is why we have prioritized the Controls and supporting Safeguards to help you plan your security improvement program. We do this through Implementation Groups (IGs). There are three IGs and are based on the risk profile and resources an enterprise has available to them to implement controls. Each IG builds upon the previous one. So IG2 builds upon IG1 and IG3 comprises all the Controls and Safeguards.

We describe a typical IG1 enterprise as small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of this enterprise is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

But no matter the size or complexity of your business, we recommend that all organizations begin with IG1. We also refer to IG1 as Essential Cyber Hygiene because it provides the actions necessary for an organization to defend itself against the major attack types being used by cybercriminals. IG1 is not just another list of good things to do; it's an essential set of steps that helps all enterprises defend against real-world threats. And it provides a strong foundation for your cyber maturity growth, or as your security needs change. This is a strong claim, but we back it up with our use of the best-available summaries of attacks (like the Verizon DBIR), and an open, shared methodology (the CIS Community Defense Model v2.0[3]).

3 https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

Stay informed and threat ready.

Facing today's threats requires intelligence from a source you can trust.

The full DBIR contains details on the actors, actions and patterns that can help you prepare your defenses and educate your organization. Get the intelligence you need to protect your organization:

Read the full 2023 DBIR at verizon.com/dbir.

Want to make the world a better place?

The DBIR relies on contributions from dozens of organizations, and we'd love to have you. If you are interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com or tweet us @VZDBIR to provide feedback for improving the DBIR. Learn more about the VERIS Framework at verisframework.org.

verizon