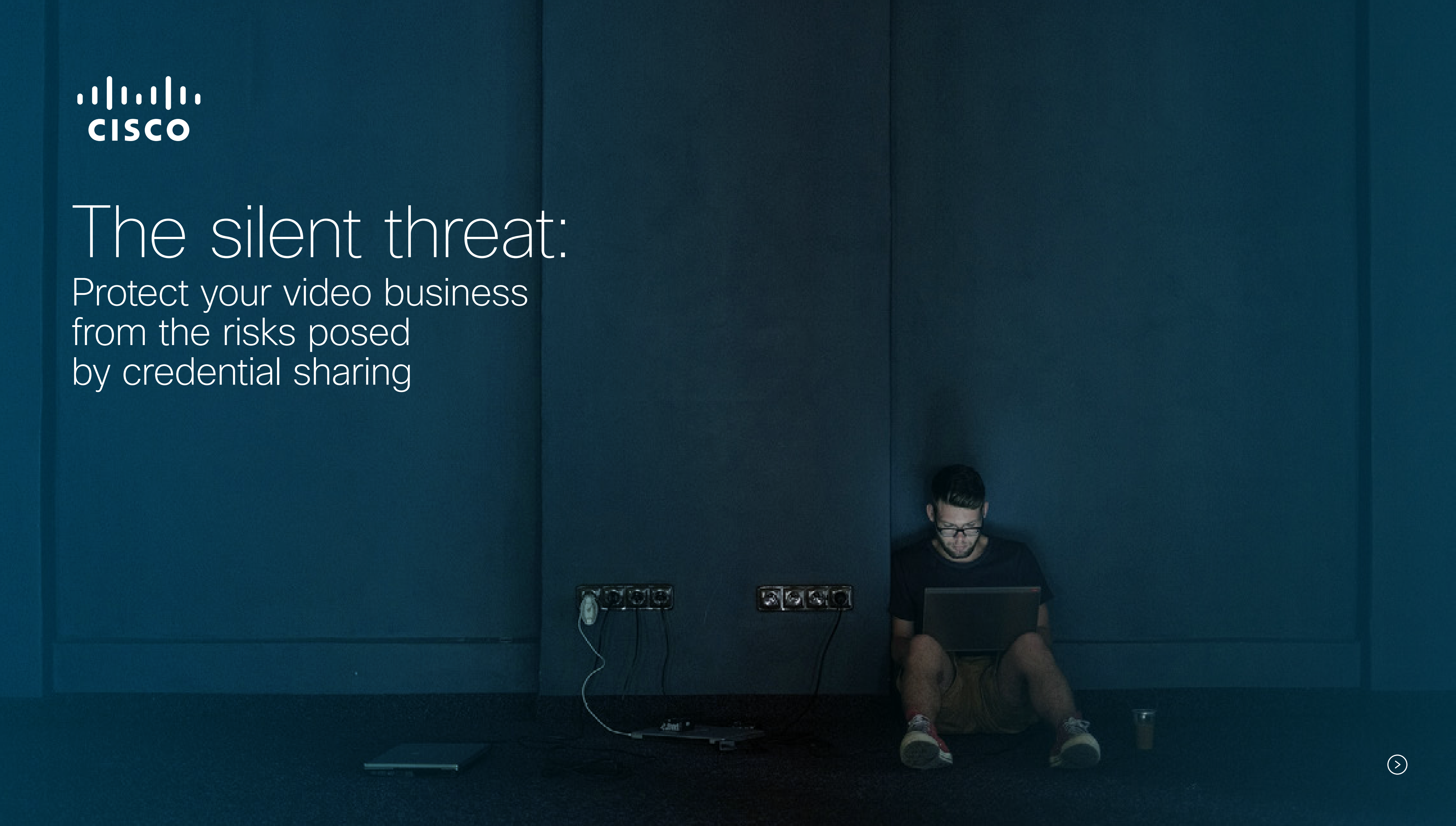


The silent threat:

Protect your video business from the risks posed by credential sharing

Contents

User credentials for video services are being shared both willingly and unknowingly. Credential sharing and theft is a multi-faceted business concern that presents many risks to your organization and your customers. Your business must not dismiss the risks posed by credential sharing.

The potential for an account holder's password to be shared is now well known. The profile of the issue continues to rise, as do the risks associated with credential sharing. In 2016 hackers stole tens of millions of customer credentials in a string of high-profile breaches. And it's not just the targeted company splashed across the headlines that suffers in these attacks. Credentials can be taken from one site or service and used fraudulently on others, so it's vital that your organization recognizes the huge damage credential sharing could do to your business and your customers. What is more, the potential risks associated to credential sharing will continue to rise as users connect more devices to the internet and rely on an increasing number of online services.

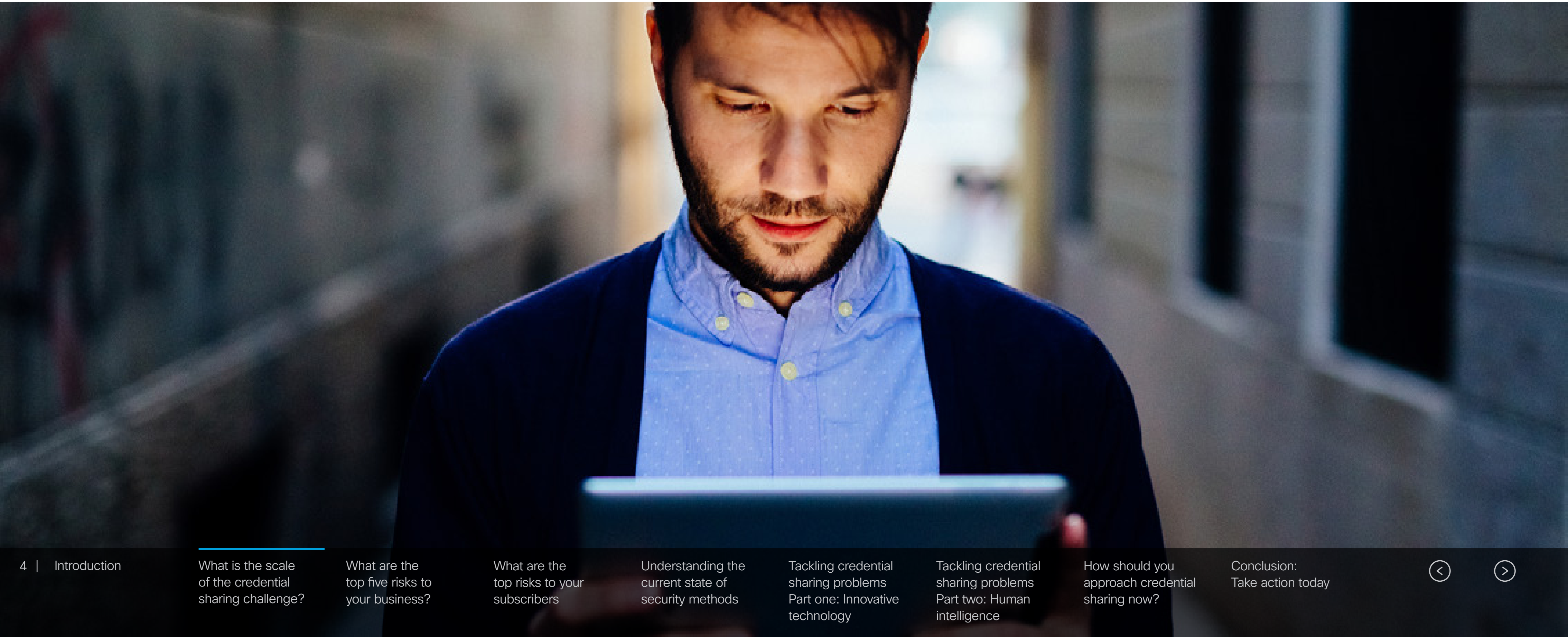
So how is your business dealing with this challenge? In many ways, the solutions for service users remain constant, such as not re-using or writing down passwords, and instead using strong passwords that are tough to break. There are, in short, some fundamentals to good security practice that haven't changed.

On the service side, however, more can be done. An important first step for your business is to gain visibility of anomalies when people access content. Such activity might include logins from unusual locations or times. The next step is to gain the ability to take proactive action against errant activity.

The good news, as we demonstrate in this eBook, is that there is a solution to the credential challenges your business faces – and Cisco can help, both in terms of technology and human expertise. By approaching the risk with careful management and strong technology, your company can overcome the challenge and help build a stronger, more secure foundation for business growth.

What is the scale of the credential sharing challenge?

01



Cisco operational security experts constantly analyze the existing and imminent content piracy threats faced by video providers. Through analysis of a range of sources including anonymized end user account information, they have identified significant business issues caused by the sharing of online video accounts.

Credential sharing occurs in a wide range of services and is a significant issue for video service providers. Cisco has identified three main types of account sharing. Understanding the characteristics of these types, and how credential sharing takes place, both willingly and unknowingly, is crucial to dealing with the challenge your business faces:

- Casual sharing: Sharing login details with family and friends
- Business sharing: Swapping account details, pooling accounts and the selling of valid or fraudulent accounts
- Stolen accounts: Stealing account credentials from legitimate subscribers in order to sell them or to access the content illegally

Let's think about the challenges associated with casual sharing. A parent, for example, might knowingly give their child access to their video service account and allow them to logon from a different location, such as their college accommodation. However, a content provider that checks account activity might view the new login as suspicious.

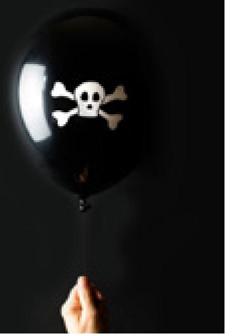
While your business might be keen to stop malicious sharing, it might also be concerned that trying to stop all forms of credential sharing – such as casually between family members – could lead to an impact on customer experience. Public positions of providers often vary; some will see casual sharing as acceptable for an amount of time and will then have a short period of cracking down.

Your business might choose to shy away from using technology to counteract the issue as they see casual sharing, particularly amongst family members, as acceptable usage. As a content provider, the last thing your business wants is to inconvenience its loyal customers while trying to stop errant account activity.

However, credential sharing creates significant problems for your business and its customers. It can be difficult to tell the difference between casual sharing and malicious activity, but the challenge is not an intractable one. Cisco has devised a solution that is described in detail later in this eBook that draws on a strong mix of innovative technology and human intelligence in order to help your business act with confidence.

Cisco operational security research on credential sharing included extensive research on both the visible web and dark web. We identified people selling stolen video service accounts on many popular ecommerce sites. Such accounts are easy to find, via a simple search, and in some cases even by browsing to sections of the sites dedicated to selling accounts. Examples of sites where we found such activity include:

- Fiverr.com
- Reddit
- bitcointalk.org
- Hackforums.net
- mpgh.net



What are the top five risks to your business?

02

So why is credential sharing a potential problem for your organization? Our research suggests five key risks are apparent.

Outages

If credentials are shared, your expectation about how many customers will be online at any time can be wrong. When a company underestimates the number of active users for any given service, their systems can, and have, become overloaded. Evidence suggests this can be a particularly significant issue during big-ticket events, such as season premieres or major live sports events. One coping strategy might be to build a scalable and on-demand IT infrastructure. Yet while such support can help prevent outages, credential sharing is likely to make the cost of such provisions much higher.

Loss of customers

Cisco has seen customers of a range of video services discussing in online chatrooms and forums their annoyance at other people using their credentials illegally to login. Stolen accounts cause problems for users who suddenly see their viewing profile has changed and their recommendations are awry. Your customer service team might provide some useful feedback but a paying client will quickly become irritated. If your business cannot ensure account integrity, then customers will be left with no sensible alternative other than to cancel their subscriptions.

Leaks of private customer data

Account security is perhaps the biggest concern of all. Privacy concerns remain a key issue in the media and with good reason. Unauthorized access to a video account is concerning enough for your business, yet credential sharing can also expose crucial personal information. The level of detail that can be accessed varies considerably and includes address information, payment plans and calling histories. No company wants to see their customer data compromised. And as recent high profile cases have shown, the damage to your brand can be compounded by the possibility of lawsuits and financial losses.

Brand reputation

If your business gets a reputation for service outages, losing customers and leaking data, then you can expect a big hit to your brand reputation. Constant inconveniences, annoyances and dangers that result from credential sharing will leave customers angry. Rather than becoming advocates for your brand, these affected customers can use online forums to vent their frustrations. Your brand must be seen to be doing everything it can to ensure its video services are available and secure.

Loss of revenue

A fall in profits can be seen as the final hit to your business. The combination of the above risks results in indirect losses. In addition, there are direct losses caused by potential customers who gain unauthorized access, instead of taking a legitimate subscription. Content providers are best positioned to estimate such losses, but clearly they have the potential to represent increasingly large sums. Estimates suggest content providers lost as much as $500m in 2015 due to credential sharing, according to research from Parks Associates.

What are the top risks to your subscribers?

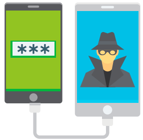
03

Credential sharing presents huge risks to your business in terms of both its reputation and its finances. Yet your customers can also suffer as a result of credential sharing – and the impact can extend a long way beyond video services.

As we noted in the previous section, a typical account for an online service includes extensive information about the account holder. Such details typically cover three key areas:

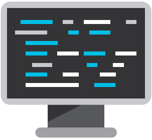
- Personal identifiers, such as home address and phone number
- More confidential data, such as viewing histories and purchases
- Financial data, such as payment methods, credit card information and bank account numbers

Your business and its customers must understand that the risks associated to credential sharing do not just stop at unauthorized access to video services. Cisco research highlights how credential sharing for one video service account can provide a gateway to other online and offline platforms, as we see next.



Privacy breaches

Cisco research has identified examples of accounts for content providers being sold for just a few dollars online. While such credentials might have been sold for the express purpose of watching media, a third-party may also decide to take a closer look at some of the personal details and services attached to the account. Cisco has found evidence of video account credentials providing access to other online services from the same provider, such as Internet of Things services. So an account purchased for just a few dollars may provide access to the security cameras, door locks, alarm systems and smart devices located in the account holder's home.



Compromised payment methods and financial loss

Cisco investigations have also revealed that multiple account types associated to video services present partial payment details that would make targeted phishing very simple. Some accounts even permit re-using previous payment methods without requiring any further verification. The implementation of such features to increase usability is understandable. But there is a trade-off in that re-usability increases potential risks that could result from credential theft. Customers must be aware of that risk and your business must do everything it can to ensure payment methods are not compromised.

Breach of other services sharing the same credentials

As mentioned above, account details acquired through credential sharing can provide a gateway point to other services. Cisco has discovered that a thief who steals a user's login details for video content will typically try to access other services with the same credentials. As people frequently re-use credentials across accounts, the breach often does not end with the initial targeted service. So if cyber criminals gain access to credentials in one account, the extent of damage they can do is way beyond that one service.

Understanding the current state of security methods

04

Cisco research suggests that existing security policies around account logins are dominated by reactive techniques. It is typical for unauthorized account accesses to be discovered by end users, rather than the service provider who should be safeguarding the account.

Following such a discovery, customers commonly approach the service provider and receive rudimentary security tips, such as how to choose a strong password. However, research shows that people have ignored this best practice tip for years – and, as data dumps from cyber criminals stealing passwords show, they continue to ignore such advice today.

So the existing, reactive approach taken by providers is insufficient. If the above approach sounds familiar, then your business must do more to help protect its services, its data and its customers. The current state of security methods is failing for a number of key reasons:

- Detection of a breach takes too long
- Breaches are generally noticed by end-users, when it is clearly preferable for the providers to be proactively monitoring for them
- Users who engage in casual sharing will not reveal the breach
- Resolving the situation requires active participation of the end users

Your business needs a more nuanced approach to the many concerns associated with credential sharing. The current solutions in the marketplace will not help you deal with the challenge effectively. What your business must strive to discover is a strategy for dealing with the wide spectrum of credential sharing in the best possible way.

The most effective approach, as we will see in the next section, is the integrated use of innovative technology and human intelligence. Credential sharing will remain a big business problem unless you draw on both techniques.

How can you tackle the credential sharing problem?

05

Part one: Innovative technology

Security tools and techniques available today can be applied to help your business deal with the credential sharing challenge. Cisco has been developing analytics and machine learning processes that provide complete visibility on credential sharing activity in your network and which enable you to take proactive action against credential sharing. Our methodology spans four key stages:

Stage one: Detection

Understanding when and where sharing is taking place, detecting suspicious account access activity

Stage two: Classification

Classifying credential sharing into one of the three key types – casual sharing, business sharing and stolen accounts – and continuously making attempts to improve this classification process based on feedback

Stage three: Scoring

Calculating how likely it is that the identified activity is associated with one of the three types of credential sharing, and then establishing the thresholds in regards to how to behave in the event that a particular type of credential sharing is identified

Stage four: Policy

Creating a plan of action for each type of activity that is identified, so that the challenges and actions per-sharing type are set in place

The crucial factor is that the innovative technology you use should help your business identify incidents of sharing; the type of sharing taking place; and it should help your organization to take proactive steps. Data science should help generate likelihood scores for every login into a system. Using these scores can help your business ascertain whether a login is coming from the account holder or a sharer who should not be accessing the account.

The technology should then allow you to enact a policy of action based on the data analysis. One response in policy terms, for example, might be a prompt for more information.

If the detection, classification and scoring process indicates that an account has been compromised, the policy might direct the login process to ask a question that only the account holder will know the answer to, such as a query relating to personal details or content viewing choices.

A technology partner such as Cisco can create a technical solution that will help protect your organization and its customers from errant activity. This system draws on big data to identity incidents of sharing, classify the types of activity and enable you to take immediate, proactive action.

How can you tackle the credential sharing problem?

06

Part two: Human intelligence

A truly all-encompassing approach to the credential sharing problem goes beyond tools. A complete solution uses domain expertise in the video space to fine-tune the system and to continually provide even better results in the fight against credential sharing.

Cisco's comprehensive approach uses human intelligence in combination with machine learning technology to create a rigorous detection and prevention strategy.

Cisco investigates who is selling credentials, ascertaining where they are selling, and understanding what types of information they are selling. Cisco's security specialists undertake these activities in multiple languages across every type of account.

Cisco research has helped demonstrate that there is a market for all kinds of credentials, even those that are free. An in-depth awareness of the credential sharing challenge does not come from simply tracking and tracing logins via technology. A full picture of the challenge comes from analyzing the market, identifying the problem and using appropriate tools to take remedial action.

Your partner must, in short, be able to combine innovative technology with detailed intelligence. Cisco's proactive, global team of security researchers and technology experts has a track record of ensuring Cisco's technological solutions stay ahead of cyber criminals, and will provide intelligence to continually refine algorithms that spot and prevent account sharing.

Partner checklist:
What type of expertise should you be looking for?

- ✓ Gathering intelligence proactively
- ✓ Monitoring illicit activities
- ✓ Identifying future hacking trends
- ✓ Exploring new realms and services for controlling piracy
- ✓ Intimate knowledge of cyber criminals' world

How should you approach credential sharing now?

07

There might be reticence in your business to challenge the issue head-on in case you impact the customer experience of individuals who knowingly share their details through casual sharing. However, the risks associated to credential sharing should be a key concern for content providers.

As we have seen in this eBook, malicious activity through credential sharing can lead to negative effects for your business and its customers. Businesses that take a proactive stance, and who work with trusted partners, are likely to be rewarded.

Here are four steps that can help shape your approach.

1. Don't dismiss the issue: You might believe credential sharing has a minimal effect on your bottom line but even the smallest number of compromised accounts can have a huge impact on your business. The combination of potential service outages and data leaks can lead to long-term damage to your brand's reputation and its revenue.
2. Look inside your operation: You might think your business is already doing enough work in regards to credential sharing but no executive can afford to be complacent. Take action to understand the scope of the problem, gaining visibility and awareness on the extent of credential sharing in your particular business.
3. Reach out to a technology partner: The right tools can be a first crucial step in dealing with the credential sharing challenge. Look for a partner with video security expertise that can help your business detect various types of credential sharing and take proactive action.
4. Use human intelligence: Technology alone will not be enough. Your partner must also specialize in human intelligence around undercover trends and emerging threats. They must use video security intelligence to make the credential sharing protection solution more effective.

Conclusion:
Take action today

Credential sharing presents a significant challenge to your video business but the issue is not intractable. Most importantly, your organization needn’t face the challenge alone. Engage with Cisco as your video security partner. We understand the problem and are already using innovative technology combined with human intelligence to develop a proactive response to varied forms of piracy, including credential sharing.

Find out how Cisco can keep your valuable video content safe

Secure your video business