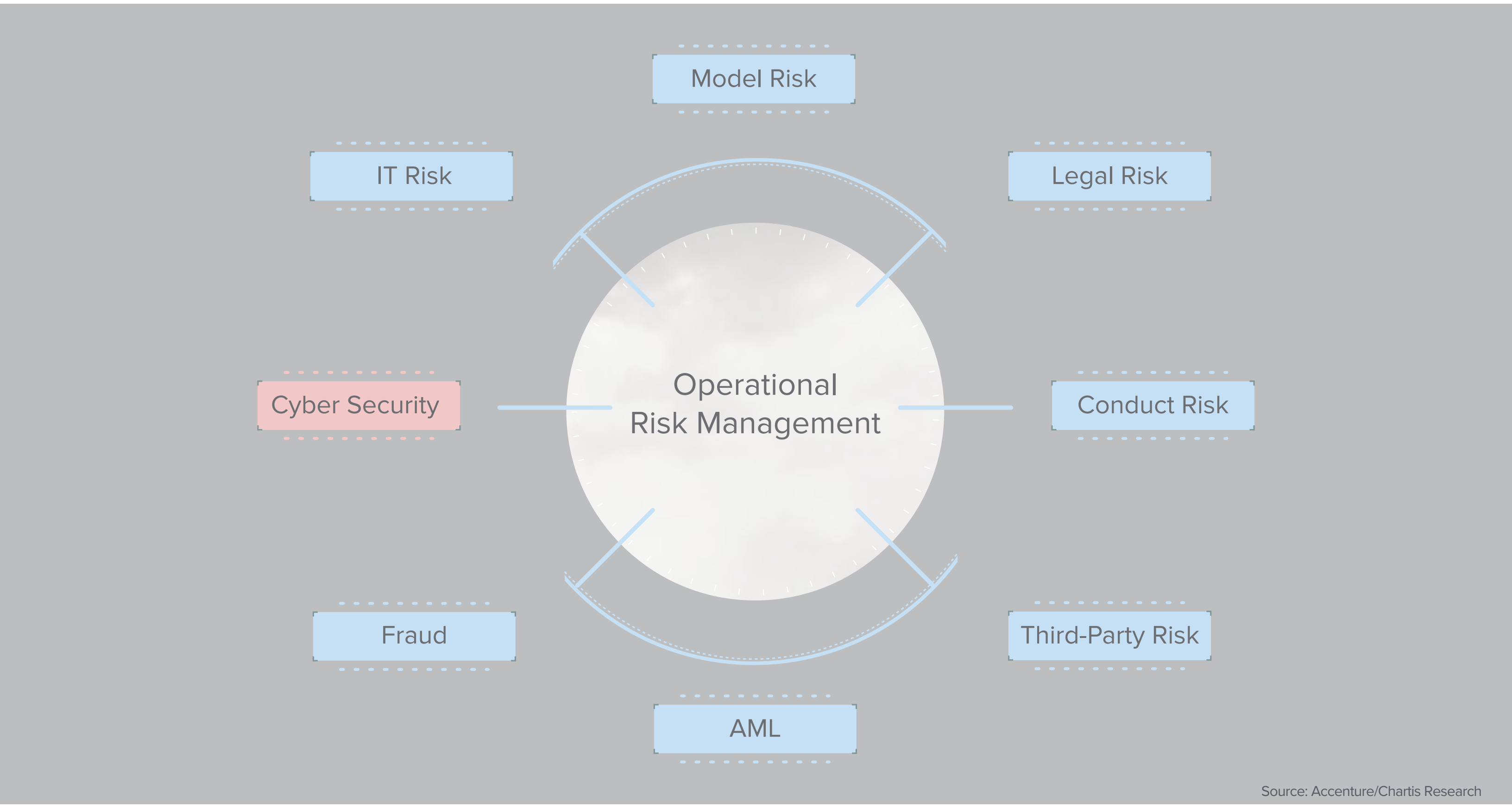
WHITEPAPER



Source: Accenture/Chartis Research

Assessing The Risk of Compromised Credentials to The Enterprise

Businesses today face an abundance of organizational risk. These come in the form of creating the business model itself, dealing with third parties, managing vendors and partners, monitoring internal and external fiscal fraud, exercising premise security and the like. In the 21st century, no greater risk is posed to the enterprise than that of risk to the technology infrastructure in the form of cybersecurity risk.

Within the cybersecurity risk itself, there are many different risks. In this paper, we will focus on Identity Threat Management and the risk of compromised credentials, which try to answer two key questions: “How at risk are my users” and “How at risk is my organization to the risk of compromised credentials.”

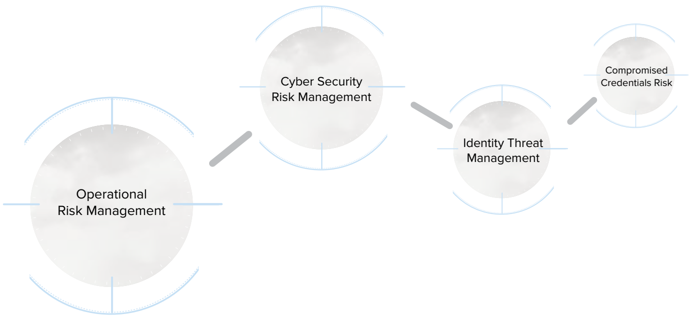


Figure 1: Identity Threat Management as part of the Operational Risk Management

CYBERSECURITY RISK & IDENTITY THREAT MANAGEMENT

Because technology now has broad and pervasive impact on the successful operation of the business, comprehensive and accurate assessment and mitigation of cybersecurity risk is absolutely essential and covers many areas of technology.

Perhaps no area of cybersecurity risk is more significant than that of Identity Threat Management as businesses ultimately harness the work of individuals who assume electronic identities within the technology infrastructure to drive the business forward. Threats to identities within the enterprise therefore are ever evolving as identities provide access to business information in the form of access to critical applications and their associated data.

Threats to identities and unintended access have been leveled at enterprises as long as identities have existed in the form of password grabbers, phishing, malware, impersonation, identity fraud, social engineering and the like. Password management, privileged access management, identity governance, and identity and lifecycle management have all been accepted ways of mitigating the many varied threats to identities, access and data.

Past known threats, however, are not finite threats to identities, access, and data. Recently, a new and pernicious threat to identities has emerged in the form of compromising the credentials of those identities. Addressing *all* threats to identities, including compromised credentials that pose enormous risk to organizations, represents a class of threat management within cybersecurity risk identified here as **Identity Threat Management**.

COMPROMISED CREDENTIALS RISK MANAGEMENT

Compromised credentials are exact match of your employees' or customers' user IDs and passwords and are available to anyone on the outside via the Dark Web[1]. Because compromised credentials represent exact match credentials, are easily obtainable from the outside, and difficult to detect, they represent a very serious and pernicious threat to organizations.

The risk associated with compromised credentials lies not only in the threat of easy-to-obtain, unauthorized entry into organizations from the outside. The risk is magnified because compromised credentials actually upend many of the traditional risk mitigations organizations typically use and rely upon to bring assurance.

THREAT TO TRADITIONAL PASSWORD MANAGEMENT

The first threat to consider is toward traditional password management. Most organizations have and enforce policies around password complexity as well as frequency and causation of resets. Compromised credentials side-step these policies since exact match means password complexity does not matter. An exact match on a complex password is still an exact match.

Frequency of password resets[2] is also affected in that forcing password resets can actually accelerate use of reused credentials in organizations and can reset the risk profile to a higher level. This potentially elevates the cybersecurity risk through in-house processes aimed at eliminating operational inefficiencies via traditional services such as self-service password resets.

THREAT TO IDENTITY VERIFICATION SERVICES AND MULTI-FACTOR AUTHENTICATION

Exact match also makes compromised credentials a serious threat to identity verification services as well as multi-factor authentication (MFA). Many organizations continue to take pedestrian approaches to identity verification and password reset (such as through secondary email validation) and MFA. Often organizations perceive these mechanisms as "silver bullet" mitigations of threats to identities and universally accept these approaches to authentication (AuthN)[3] and authorization (AuthZ)[4] mechanisms as sufficient assurance.

[1] Dark Web – used as an aggregate term for dark web, deep web and surface web

[2] Not withstanding the fact NIST has already determined past policies around traditional password reset policies not only does not lower risk, but in fact likely increases it. See new NIST 800-63-3 Guidelines.

[3] Authentication (AuthN): Determining identity – is a business entity who or what it claims to be?

[4] Authorization (AuthZ): Determining a given identity's access – does or should an authenticated identity have access to a technology asset?

When an attacker has a valid set of compromised credentials in hand, those credentials can often be leveraged to easily defeat commonly accepted identity verification mechanisms and circumvent MFA through disablement, interception or social engineering.

SCORING COMPROMISED CREDENTIALS RISK

To ascertain and score compromised credential risk, the following approach is intended to provide risk officers within an organization with a way to accurately measure risk and to subsequentially formulate a defense strategy through commonly accepted cybersecurity frameworks as part of its cybersecurity risk Management.

The metrics used to score compromised credentials risk is as follows: **Percentage of Compromised Credentials**, taking into account types of credentials; **Availability of Compromised Credentials** as not all credentials on the Dark Web are available at once; and **Percentage Convertible to Plaintext Credentials** as both the ability to readily convert an organization's passwords to plaintext as well as the additional intelligence plaintext provides increases the likelihood of a successful attack.

PERCENTAGE OF COMPROMISED CREDENTIALS

Every organization at any given time has a finite pool of credentials. The Dark Web has a large and growing pool of compromised credentials. There is a likelihood some of those user IDs and passwords to be exact match with credentials at your organization. How many matches (leaked credentials) your organization has divided by your total pool of credentials is "a" percentage.

Privileged credentials, even if only one or a few, pose enormous risks to organizations. To quantify this risk assessment, we are estimating the risk of privileged credentials as ten times the risk of a non-privileged, normal user credential. Each organization should determine what that number is based on the breath of privileges of its privileged user accounts and the level of damage an attacker, possessing such credentials, can do to the organization. Similar process should be followed for determining the risk multiplier for the non-user IDs.[5]

Recommended is a weight of ten (10) for privileged credentials, five (5) for non-user ID and power user credentials, and one (1) for non-privileged credentials. The resulting equation for determining percentage of risk with weight is then as follows:

$$\frac{(1N+5N+10N)}{T} = \textit{Aggregate}\ \%$$

Where N is the total number of compromised credentials per type (weight) divided by T, the total number of credentials an organization has. Then aggregate percentage becomes the overall percentage of compromised credentials and is risk scored linearly.

Percentage of Compromised Credentials	Risk
> 70%	Maximum
51% - 70%	Very High
31% - 50%	High
11% - 30%	Medium
< 11%	Low

Bear in mind, *any* compromised credential poses significant threat to the organization since *any* access represents at least a beachhead into an organization's technology infrastructure. This is one reason why non-user IDs, which typically exist in an unmonitored and unaccounted-for state, pose more risk than a non-privileged, normal user credential.

AVAILABILITY OF COMPROMISED CREDENTIALS

Not all leaked credentials are available on the Dark Web all the time. The Dark Web is like a food bazaar on a busy street in Bangkok — all kinds of credentials are offered and then suddenly made unavailable for various reasons.

Some buyers want exclusive access to types of credentials based on perceived value. For instance, credentials of a certain class or type, such as leaked credentials from a financial institution, will more likely be perceived as high value since individuals will often create credentials of a certain kind and then reuse those same credentials across all their financial accounts, but not with their social media accounts.[6]

[5] IDs created for non-user accounts such as application IDs, testing IDs, FTP IDs, layered product IDs, etc.

[6] There exists a very real sense in which credentials get "risk scored" and categorized at the moment of password creation by the users themselves. This greatly aids the underworld in terms of first level analytics around value, vector and probability.

Availability is based on two factors: firstly, *if* a compromised credential has been available and secondly, how *long* it's been available. If a compromised credential is no longer available, but experienced "some" availability, then the risk is lower. If a compromised credential is currently available and has been for some time, then the risk is higher.

As data breaches with compromised credentials are the most prevalent attack vector[7], the risk around availability is relatively linear and deterministic with the overall risk score for an organization based on aggregate risk of any and all compromised credentials found through a trusted compromised credentials intelligence source.

Available Now?	Has Been Available	Risk
Yes	3 months or longer	100%
Yes	More than 2 weeks but less than 3 months	80%
Yes	Available for the last 2 weeks	60%
No	3 months or longer	50%
No	More than 2 weeks but less than 3 months	30%
No	Available for the last 2 weeks	10%

PERCENTAGE CONVERTIBLE INTO PLAIN TEXT

Finally, the percentage of passwords an organization has that are easily convertible to plain text is an important indicator of risk.

When passwords are presented to a trusted compromised credentials intelligence source such as VeriClouds as seed data to analyze and find compromised credentials, those passwords are typically checked by the service to see how easily they can be converted to plain text.[8] Any success greater than 20% is considered high risk to an organization. In this case, length and complexity do actually matter.

The risk around percentage convertible into plain text is also relatively linear and deterministic and can be provided based on an overall aggregate score through use of a trusted compromised credentials intelligence source.

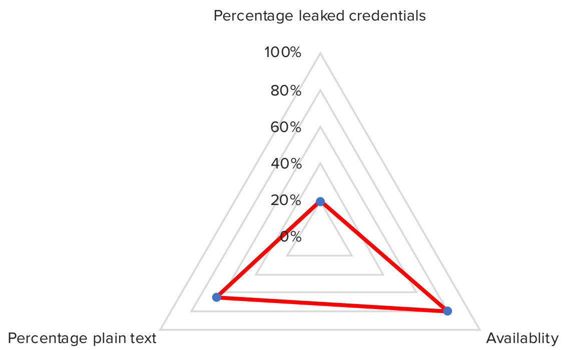
Percentage of All Credentials Convertible	Risk
>= 85%	Maximum
51% - 84%	Very High
21% - 50%	High
1% - 20%	Medium
0%	Low

RISK SURFACE

Once all risk scoring for compromised percentage, availability and plaintext percentage is known, then the scores can be triangulated according to the three points in a spider chart to visualize the total risk surface. The greater the risk surface, the greater the aggregate risk to an organization.

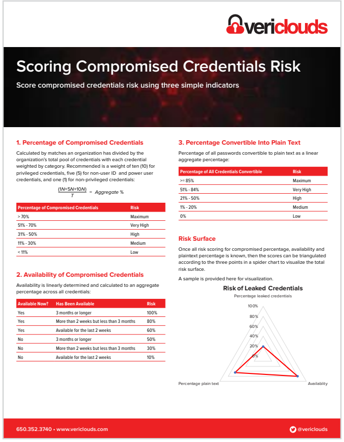
A sample is provided here for visualization.

Risk of Leaked Credentials



DOWNLOAD SCORING GUIDELINES

In an effort to jumpstart your organization in assessing your actual cybersecurity risk in the area of Identity Threat Management for compromised credentials, visit this link, or click on the page thumnail below to download a concise PDF formatted version of the scoring approach described.



vericlouds

Scoring Compromised Credentials Risk

Score compromised credentials risk using three simple indicators

1. Percentage of Compromised Credentials

Calculated by matches an organization has divided by the organization's total pool of credentials with each credential weighted by category. Recommended is a weight of ten (10) for privileged credentials, five (5) for non-user ID and power user credentials, and one (1) for non-privileged credentials:

$$\frac{(1N+5N+10N)}{T} = \textit{Aggregate \%}$$

Percentage of Compromised Credentials	Risk
> 70%	Maximum
51% - 70%	Very High
31% - 50%	High
11% - 30%	Medium
< 11%	Low

2. Availability of Compromised Credentials

Availability is linearly determined and calculated to an aggregate percentage across all credentials:

Available Now?	Has Been Available	Risk
Yes	3 months or longer	100%
Yes	More than 2 weeks but less than 3 months	80%
Yes	Available for the last 2 weeks	60%
No	3 months or longer	50%
No	More than 2 weeks but less than 3 months	30%
No	Available for the last 2 weeks	10%

3. Percentage Convertible Into Plain Text

Percentage of all passwords convertible to plain text as a linear aggregate percentage:

Percentage of All Credentials Convertible	Risk
>= 85%	Maximum
51% - 84%	Very High
21% - 50%	High
1% - 20%	Medium
0%	Low

Risk Surface

Once all risk scoring for compromised percentage, availability and plaintext percentage is known, then the scores can be triangulated according to the three points in a spider chart to visualize the total risk surface.

A sample is provided here for visualization.

Risk of Leaked Credentials

Percentage leaked credentials

100%
80%
60%
40%
20%
0%
Percentage plain text
Availablity

650.352.3740 • www.vericlouds.com

@vericlouds

DOWNLOAD NOW

Of course, again, use of these scoring guidelines requires access to intelligence through a trusted compromised credentials intelligence source to determine whether or not your organization has compromised credentials, which ones are compromised and totals. But once this intelligence is obtained, the risk can be readily identified through the process outlined herein.

[7] 81% of reported data breaches are the result of weak or stolen credentials, *2017 Verizon Databreach Investigations Report*

[8] Success of converting passwords to plain text depends on the hash used, whether they are salted and the length and complexity of the password.

FRAMEWORK FOR COMPROMISED CREDENTIALS LINES OF DEFENSE

Once an organization has workable metrics around scoring the cybersecurity risk of compromised credentials, it can plug those metrics into many of the well-known cybersecurity frameworks available for assessing and mitigating that risk through lines of defense and use of tactical measures. A Basel Framework is discussed here as an example.

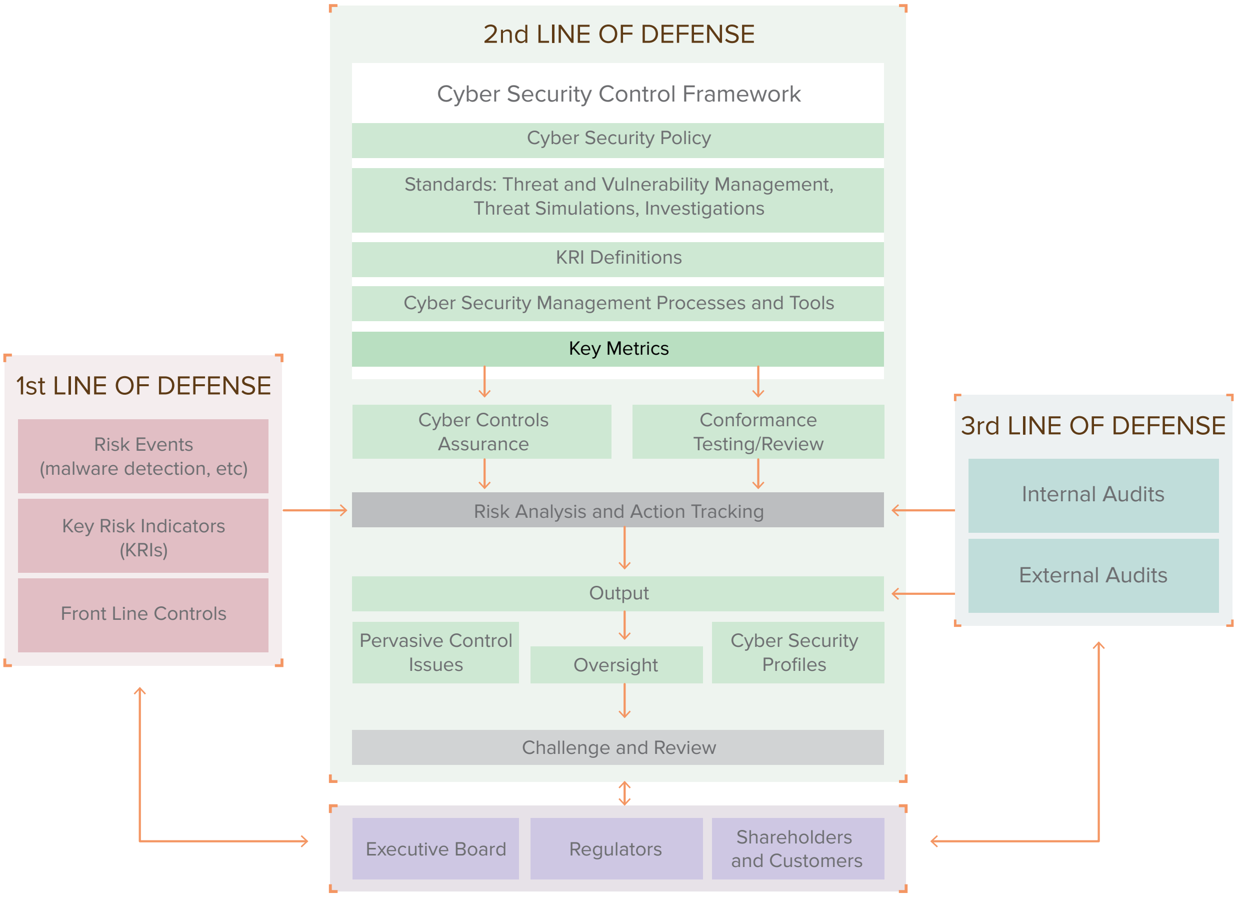

2nd LINE OF DEFENSE
Cyber Security Control Framework
Cyber Security Policy
Standards: Threat and Vulnerability Management, Threat Simulations, Investigations
KRI Definitions
Cyber Security Management Processes and Tools
Key Metrics
Cyber Controls Assurance
Conformance Testing/Review
Risk Analysis and Action Tracking
Output
Pervasive Control Issues
Oversight
Cyber Security Profiles
Challenge and Review
1st LINE OF DEFENSE
Risk Events (malware detection, etc)
Key Risk Indicators (KRIs)
Front Line Controls
3rd LINE OF DEFENSE
Internal Audits
External Audits
Executive Board
Regulators
Shareholders and Customers

Figure 2 - Basel Framework for aligning operational risk with cybersecurity. Source: Accenture/Chartis Research

First Line of Defense: Risk Events, Risk Indicators & Front Line Controls

Risk Events for compromised credentials are simply the positive occurrences of compromised credentials to an organization. This indicates compromised credentials exist.

The Risk Indicators are the scoring metrics already laid forth in **Scoring Compromised Credentials Risk**.

Front Line Controls for compromised credentials is use of a trusted compromised credentials intelligence service that allows tactical implementation of both active and passive technical use cases within IAM to provide real-time and batch implementation for compromised credentials mitigation.

Second Line of Defense: Cybersecurity Policy, Management & Key Metrics

Cybersecurity Policy for an organization needs to define the risk from compromised credentials, stipulate that compromised credentials will not be allowed, and how compromised credentials will be mitigated and disallowed at the tactical level through defined technical use cases.

Management of compromised credentials need to take place at the tactical level that exist through implementation of technical use cases stipulated in the Cybersecurity Policy.

Key Metrics used to measure and report the effectiveness of both the policy and management of compromised credentials are the metrics again defined in **Scoring Compromised Credentials Risk**. Over time, the risk surface within an organization through policy and management should show a greatly reduced attack surface.

Third Line of Defense: Internal Audit

Internal Audit is an implemented process that checks on a regular basis to insure the policies, management, and mitigating controls for compromised credentials have been implemented, remain implemented, and that appropriate actions stipulated in the policy have been taken.

ASSESSING THE RISK OF COMPROMISED CREDENTIALS

Compromised credentials are a rapidly emerging and dangerous risk to organizations that require senior cybersecurity and risk officers within to take notice, assess and sufficiently address. It is hoped this paper helps highlight, articulate, and provide proper guidance in scoring, assessing and building lines of defense through accepted cybersecurity frameworks to mitigate this risk.