Brand Protection
De La Rue

Lessons from Cyber-security Resiliency to apply to our COVID-19 Response

May 2020

Sherri Erickson, Key Account Director

De La Rue

Lessons from Cyber-security Resiliency to apply to our COVID-19 Response.

Sometimes when we're faced with a novel challenge, it's helpful to use what we've learned in the past and apply those insights and approaches to help us solve for the new problem. What isn't immediately obvious may reveal itself as we shift our context to look at the situation in a new light.

This article does not presume that I have the answers to solve the global pandemic from COVID-19; my hope is that it inspires people to think differently about what they can do to ensure life-saving solutions reach those who need them most.

What are those lessons from the past?

There is a 0.79 correlation between use of unlicensed software and malware encounters. This was established in 2015 when IDC published a whitepaper, "Unlicensed Software and Cybersecurity threats" based on a study sponsored by BSA| The Software Alliance. To put this into perspective, the correlation between education and income is 0.77, between anti-corruption policies and economic growth is 0.77, and between smoking and lung cancer is 0.72. For further context, a perfect correlation would be 1.0 and 0 means no correlation whatsoever.

Eye opening, especially when we see cigarette packaging with graphic illustrations and explicit verbal warnings that cigarettes kill, cause birth defects, and can lead to blindness, amputation and other fatal diseases. This, with a correlation that's nearly 10% lower than that of malware and unlicensed software.

Unlicensed software is comprised of both counterfeit software and software that's been installed in an environment where it's not supposed to be deployed.

Counterfeit is a known, proven, evidence-based carrier of bad stuff that bad actors regularly infuse with Trojans, viruses, worms and the like, regardless of how it is distributed.

Security experts and numerous studies have warned that downloading unlicensed software is among the highest probabilities of ways to get infected, as happened with the "Conficker" worm back in 2008/2009;

and in the Citadel botnet, criminals had pre-infected unlicensed Microsoft Windows and created 5 million zombie computers across 90 countries.

Unlicensed software in an enterprise organisation may itself not carry malware, but organisations that do not have policies, processes, systems, and controls over their software deployment practices are at risk of introducing unlicensed or counterfeit into their environments.

The study went further to define how accurately one could predict malware encounters from use of unlicensed software, and determined there is a strong ***predictive*** value of 0.62, and, further, it established there is strong empirical evidence of a ***causal*** relationship. For details on all the above, you can read the whitepaper, available through IDC or BSA |The Software Alliance.

Behind the scenes of this study are details on the strongest drivers and predictors that contribute to the correlation. These indicators, when applied to the model, will help best predict the strength, or weakness, of an environment that is best able to protect against malware. Listed in order of strength, the below indicators together provide the clearest picture of whether a country will have a higher or lower correlation. It should be noted that adding more indicators does not increase the predictability. They are:

1. Customs enforcement of software piracy
2. Customs sanctions and procedures for software piracy
3. Government use of licensed software
4. BSA piracy rate
5. Public perception of risks associated with unlicensed software
6. Channel perception of risk associated with unlicensed software
7. World Economic Forum IPR ranking
8. Compliance with international copyright treaties
9. Civil sanctions for software piracy

Why is this relevant today?

The collective global response to COVID-19 has been nothing short of miraculous, and more and more industries and organizations are stepping up to provide solutions. Historically these products have not been a target for counterfeiters, so understandably they've not developed strategies or implemented protections and now they're an easy mark.

A lot is going right, a lot more needs to be done, and there are obstacles that still need to be removed so together our comeback can be accelerated and be more effective in the long-term.

Unfortunately, bad actors are taking advantage of the pandemic. They are producing counterfeit face masks, test kits, pharmaceuticals, hand sanitizers and more. They are distributing their counterfeit products across borders, across oceans, within countries and through online marketplaces. They are abusing gaps in distribution channels, exploiting consumers who are unaware that the product is not genuine, and targeting markets where the problem is most severe. And they may be relying on not getting caught or having to face harsh penalties for their actions.

Assuming general agreement that counterfeit COVID-19 solutions are bad, let's cover what actions we might take based on what we've learned from the correlation between unlicensed software and malware.

What can we learn from cyber-security resiliency?

Leading Indicators	Application to COVID-19	Observations on COVID-19	Actions
Counterfeit is bad	Are genuine solutions identifiable as such?	Most COVID-19 solutions in market do not have mechanisms to identify them as genuine.	Brands producing COVID-19 solutions can incorporate an authentication mechanism in their packaging and promote it on their website.
Ignorance of counterfeit creates risk	Can consumers tell if a product is genuine?	Because there is no identification of genuine on the product, consumer is unaware.	
#1 Customs enforcement	Are customers actively enforcing counterfeit?	Customs are finding and enforcing counterfeit, but only what they can identify.	
#2 Customs sanctions	Are customs empowered and enabled to enforce?	Customs are enforcing, within the structure with the tools they already have.	Adding Track & Trace functionality to a Brand's authentication mechanism better enables agents with tools to enforce.
#3 Government role model	Is the gov't acting on ensuring distribution of genuine and stopping counterfeit?	No observable government priorities on enforcement of COVID-19 counterfeit.	Write to your government representative.
#4 SME global metrics of the problem	Does the CDC have the data on the scope and impact of counterfeit?	Data is captured sporadically via enforcement but not aggregated, shared, or scoped on the impact.	Adding Track & Trace functionality to a Brand's authentication mechanism enables data capture, data aggregation and data sharing.
#5 Public perception of risk	Do consumers know about counterfeit solutions and the associated risk?	Broad awareness of COVID-19 risks and actions to protect oneself, but communications do not address counterfeit.	Shared humanitarian effort by industry giants.
#6 Distribution perception of risk	Do marketplaces and channels know or have shared risk on distribution of counterfeit?	Largely enforcement and watchdog led efforts, but no cohesive, collaborative effort to address.	
#7 Industry ranking of risk	Does WHO have a ranking of countries at risk?	Scam alerts but no focus or metrics on counterfeit.	Adding Track & Trace functionality to a Brand's authentication mechanism enables data capture, data aggregation and data sharing.
#8 Government compliance with international agreements	Is the gov't aligning on a cross-border agreement to reduce risk?	Are there international agreements on response to COVID-19 counterfeit?	
#9 Civil sanctions for bad actors	Are sanctions in place that appropriately penalise bad actors in a pandemic?	Sanctions vary by country for counterfeit penalties but haven't heard of COVID-19 specific sanctions.	Write to your government representative.

Some of the above areas are more easily addressed because we're independently able to, and others may be outside our area of influence. Where you can act, do it. Where you can influence, speak up. Where you have better ideas, implement them.

To learn more about the thinking behind the scope and structure of a strategy that builds on lessons learned from cyber-security resiliency, contact sherri.erickson@delarue.com.

De La Rue International Limited
De La Rue House, Viables,
Jays Close, Basingstoke, RG22 4BS,
United Kingdom

T +44(0)1256 605000
F +44(0)1256 605196

authentication@delarue.com
www.delarue.com