Why the Human Element Matters More Than Ever

WHITE PAPER

cyberconIQ

cyberconIQ

Why the Human Element Matters More Than Ever!

By Dr. James Norrie, Founder & CEO

One of the things we most often hear from our clients – which we believe to be a common misconception – is that enhanced threat filtering and end-point security are achieving a level of effectiveness where most threats no longer even make it to our employees' inboxes. The thinking goes: instead of relying on the employee to detect and interdict a threat, simply preempt its delivery. On the surface, this argument is both valid and persuasive, but only to a point in our view.

Consider the pressing problem of ransomware attacks against this line of reasoning. It is practically true that using appropriate anti-virus filtering, accompanied by first-class intelligence that *many* vendors can keep you ahead of *most* threats. Research suggests that when this tactic is properly applied it will keep most organizations safe from 85% to 92% of the most common ransomware code at the source.

That still renders the conclusion that 8% to 15% of active new threats remain undetected at the source and still likely to reach your employees. This means an important line of defense – the last mile in your human firewall – must still be equipped to predict, detect, and interdict attacks through effective cybersecurity awareness training and deeper personal security practices. But to stop the story there would be to not fully explore the more urgent and emergent contributing human factors threats.

Multiple sources of research on threat intelligence and emerging attack vectors reveal new and sneaky tactics enabling this sharp spike in successful ransomware attacks. Through 2019 and 2020, various sources report not only a staggering increase in the volume of attempted attacks, but more depressing is an increase in both the proportion and cost of successful ransomware attacks. Last quarter 2019 data suggests the average cost of a ransomware attack is now $377,000 while the average component of ransom paid rose to $84,000. And that by 2021, these successful attacks will continue to increase to the point where projected global costs exceed $20B in economic damage[1]. This is up from less than $500M just a few short years ago. That is startling.

So, if our technology defenses have vastly improved how should this even be possible? As our perimeter defenses improve successful ransomware attacks should decline. And therein lies the most relevant findings of just how important the human component of cybersecurity is. Consider the following enablers of ransomware attacks and think about their impact on your organization:

1. Hackers are now focusing on hybrid social engineering attacks as a precursor activity against your organization to obtain administrative credentials that enable them to gain access to disable security and network security tools running on your network. If they can disable your technology, they can defeat

[1] All statistics drawn from Hashedout's 2019 "20 Ransomware Statistics You're Powerless to Resist Reading" available from **theisstore.com** and other online sources.

your security. Access is used to provide a brief window of opportunity in which to deliver the payload to your employees before restoring functionality, often undetected. This ruse is one of the fastest rising cybersecurity sneak attacks of late.

2. There is also a range of open source applications like MimiKatz that cybercriminals use to steal, view, and save authentication credentials over time. So, an attack from long ago can still haunt us today. These combinations of ID and password are retained or offered for future sale so an intruder can easily enter your network, attach the payload to an internal message, and all from inside your perimeter defenses. Now you have been hacked from inside out, not outside in.

3. A noted vulnerability often missed by cybersecurity professionals is entirely disabling the full access of former employees. Especially in larger enterprises, the employee separation process may include notifications or prompts for the suspension of a departing employee's e-mail account. However, even with strong SSO and other technologies running, many organizations still require a range of logins to multiple systems, both inside and outside the perimeter. Do your processes ensure that every single one of those system privileges has been terminated? If not, data long since stolen may enable remote system access, and worse still, might go unnoticed because the primary employee ID is removed from your network security tools meant to detect, track and deny such employee access.

In all three instances, we see how the human component is exploited by the steady, patient planning by savvy cybercriminals. And that must be occurring – or we would not be seeing the significant rise in the number of successful attacks that we are. And adding more technology will not solve a technology problem. Instead, consider an investment in your most important asset: your people. Building a deep, sustainable cyber aware culture through empowerment instead of fear – making them feel like Cybersecurity is a team sport – will advance your internal risk and compliance culture. It also has the benefit of making them personally better off because what they learn that keeps not only your organization safer but keeps them safer online at home too. And with the continuing trend of working from home, this is a dual benefit for all concerned.

Finally, we are still astonished by the sheer volume of organizations – both large and small and across a wide range of industries – that either does not know about or do not see the value in investing in employee cybersecurity awareness training. That is, until it is too late. We often get a new client *right after* they were just hacked. And that is sad for all concerned. While no security practice can offer 100% protection, an ounce of prevention is worth a pound of cure in our business!

So, reach out to us – or for that matter – even reach out to a competitor if you prefer. But do not wait until it is too late. Because people in your organization are going to be exposed to ransomware threats and technology will not save you, but human ingenuity and engagement to prevent the problem can.

For more information or to learn more about the cyberconIQ solution, please contact us at info@cyberconiq.com