LOOKING FORWARD AND LOOKING BACK:

Lookout's cybersecurity predictions

by Kevin Mahaffey

Every year, cybersecurity pundits cast predictions for which issues will make headlines in the year to come.

We've certainly contributed our fair share of these predictions.

Going forward, we're going to change the timeframe of our predictions.

Instead of assessing what the next 365 days will bring, we are going to look forward with a three year rolling window.

Major cybersecurity themes for 2016-2019

Operating systems and form factors will converge, blurring the lines between PC and mobile device

Most people define mobile devices – smartphones and tablets – as those running a mobile-optimized operating system (e.g. iOS, Android, Windows Phone). **There's a trend emerging, however, in which traditional mobile devices are gaining functionality typically associated with PCs.**

At the same time, PCs are being architected more like mobile devices – an interbreeding of species, if you will. The iPad Pro, for example, has a keyboard. With Windows 10, phones and tablets can run "Universal" apps that also run on PCs. Windows 10 also has application-layer sandboxing, code-signing, and an app store with apps pre-vetted by Microsoft. In certain configurations (i.e. enterprise-managed devices), a laptop running Windows 10 has a security architecture that looks strikingly similar to a smartphone or tablet.

We expect the blending of species to continue and cause the classic differentiators between mobile devices and PCs to (eventually) disintegrate into a difference in nothing more than screen size.

The enterprise network perimeter is going to die and be reborn

The rumors of the enterprise network perimeter's death have been greatly exaggerated. While many major breaches involve an attacker bypassing a firewall to get at valuable data behind it, most organizations still use the perimeter as a cornerstone of their security architecture.

Even when moving to the cloud, enterprises often extend their perimeter to virtual systems. Because business needs dictate having innumerable exceptions to perimeter access controls (e.g. open ports for web services, partners and contractors needing access, VPNs and Wi-Fi granting access to unmanaged devices), IT no longer effectively controls what can get behind the firewall.

We foresee "re-perimeterization", where instead of monolithic internal networks, enterprises will build micro-perimeters that protect individual applications and data stores, each enforcing its own security policy.

Cybersecurity effectiveness will be measured by risk reduction not technology deployment

In the past, increasing focus on cybersecurity meant buying “yet another box.” Deploying solutions without first understanding the problems to solve and a strategy to solve them has proven ineffective and mega-breaches have proliferated over the past few years.

Real progress, however, will come by measuring **actual** risk reduction, instead of aiming for the hollow victory of solution deployment. Cybersecurity professionals will need to show how their technical solutions have reduced risk across an organization and the companies behind those technical solutions will need to measure success based on their effectiveness.

This is a significant shift from the current paradigm that often highlights implementation over efficacy, and a lot of security vendors won’t be happy.

Enterprise-targeted iOS attacks will emerge

It’s fair to say that attackers are increasing their investment on iOS. If you view attackers as rational economic actors, investment in targeting iOS is logical, given Apple’s growing smartphone market share, currently around 14 percent globally as of Q2 2015 according to IDC. This year, for example, the XcodeGhost attack utilized trojanized versions of Xcode, Apple’s development environment, to inject malware into legitimate iOS apps when developers compiled them. Many of these infected apps subsequently made it onto the App Store.

We don’t believe that mainstream attacks from the App Store will become the norm. We do, however, foresee growth in enterprise-targeted iOS attacks given the large amount of data stored on and accessible to enterprise mobile devices and the high prevalence of iOS devices in enterprise environments. It’s highly likely that enterprise targeted attacks on iOS will be conducted via a combination of malicious apps, exploitation of vulnerabilities in legitimate apps, operating system exploitation, and end-user social engineering.

Your phone will become more important than your password

YOUR PHONE WILL BECOME MORE IMPORTANT THAN YOUR PASSWORD

The password is possibly the single largest security problem on the Internet today. Weak passwords, individuals re-using passwords across sites, and password resets being available to anyone with access to your email all contribute to the password being an Achilles heel in even a very paranoid person's security posture.

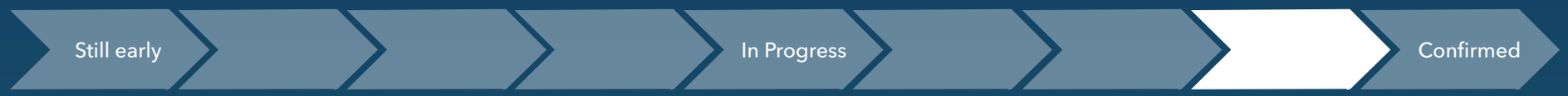
Increasingly, individuals and organizations are adopting password managers and multi-factor authentication technologies to plug some of the holes in password-based authentication.

Going forward, we foresee a world where practically everyone uses their smartphone as a multi-factor authentication element. In this world, the smartphone becomes your most valuable asset: both something that enables you to unlock your life online and a target for attackers seeking to access your services.

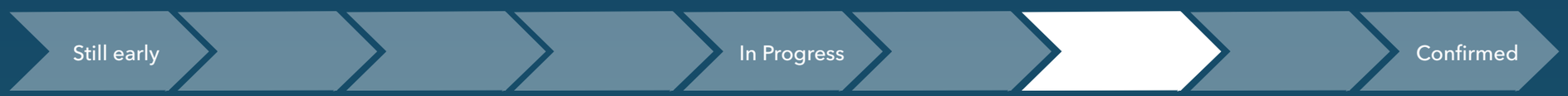
We also decided to look back at our past predictions to see what we got right and where we were wrong so we can get better in future years.

Looking Back on Lookout's 2015 Predictions

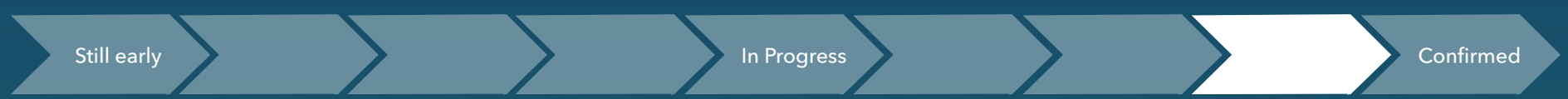
There will no longer be a technology industry. All industries will be technology industries.



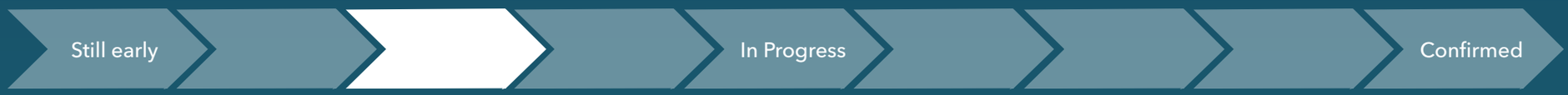
Cybercrime will just be called crime



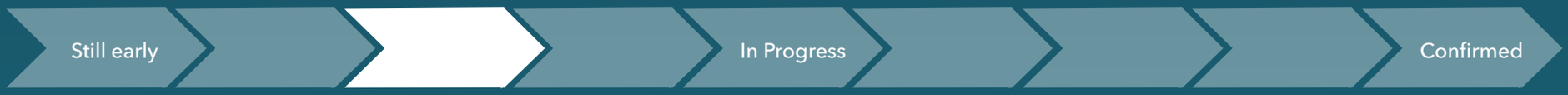
Mainstream iOS attacks will increase



Pre-installed malware will increase



Vulnerable apps will become a bigger problem than vulnerable operating systems



Privacy concerns will head to the enterprise

United States will become more of a target for mobile malware

The year isn't over for this one. We'll have more to share in January when we release our Mobile Threat Report.

Internet of Things/wearable devices will not be a priority for cybercriminals… yet

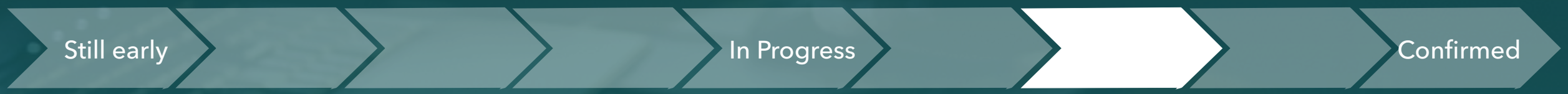
There will no longer be a technology industry.
All industries will be technology industries.

There used to be a clear line between tech and other industries; however, we are increasingly living in a world where every company must become a technology company to compete.

Taxis are dispatched from your phone, restaurants use apps to speed up the take-out process, and many other industries are improving their customer experience by digitizing it.

Furthermore, we're seeing industries go mobile, as many of these innovations happen on a smartphone, not a PC.

Cybercrime will just be called crime

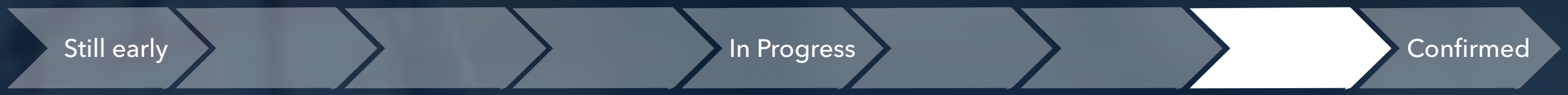


The line between “crime” and “cybercrime” is blurring.

Take, for example, car thieves taking advantage of keyless entry systems to steal cars.

As technology pervades everything, digital breaches will become so frequent that the “cyber” part of crime will be a given.

Mainstream iOS attacks will increase



Between XcodeGhost, a repackaged version of Apple's legitimate developer tool that inserted malicious code into unsuspecting developers' apps that were published on the App Store, and XAgent, iOS side-loaded malware that reportedly targeted western companies and governments, attackers are clearly stepping up their focus on iOS devices.

** This prediction is evolving. See how in our 2016 prediction, Enterprise-Targeted iOS Attacks Will Emerge.*

Companies will replace reactive security with predictive security

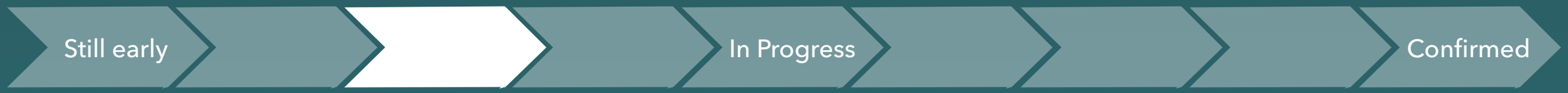
Many organizations understand that signature- and behavior-based detection require an attempted attack to have already taken place. Most don’t have the data gathering and analysis systems in place to move towards a data- and risk-driven, predictive security model.

Pre-installed malware will increase

While malware preinstalled at the factory occurred a number of times in 2014, we did not see an uptick in 2015.

Instead, attackers turned to using local privilege escalation exploits (rooting) to gain system access and prevent their malware from being uninstalled.

Vulnerable apps will become a bigger problem than vulnerable operating systems

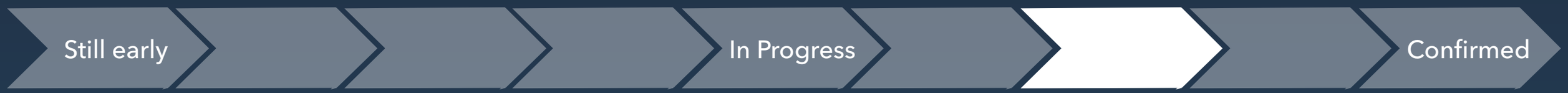


Many mobile applications are not built with security in mind and, once they are deployed, much harder to patch than an equivalent web application.

The shift from web applications to mobile applications at many organizations, however, is still in its infancy. Many enterprise workflows remain inaccessible to mobile users.

As the inevitable push to mobilize continues, we remain concerned that mobile application vulnerabilities will present a large problem to organizations in the future.

Privacy concerns will head to the enterprise



The U.S. Office of Personnel Management (OPM) hack is a prime example of why employees are (rightly) becoming concerned over what data their employer collects and stores about them.

Both governments and private organizations are needing to take important steps to minimize the data they collect and better protect the data they need to keep around.

United States will become more of a target for mobile malware

Still early | In Progress | Confirmed

The year isn’t over for this one. We’ll have more to share in January when we release our Mobile Threat Report.

Internet of Things/wearable devices will not be a priority for cybercriminals… yet

This still holds water. With the exception of industrial IoT (e.g. manufacturing, the smart grid, nuclear facilities), consumer IoT is still a relatively uninteresting vector to cybercriminals.